Sun™ Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 820-6410-10
December 2008, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Copyright © 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.sun.com/patents and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, Sun Blade, Sun Fire and docs.sun.com are trademarks or registered trademarks of Sun Microsystems, Inc., or its subsidiaries, in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse http://www.sun.com/patents et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, Sun Blade, Sun Fire et docs.sun.com sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc., ou ses filiales, aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont regis par la legislation americaine en matiere de controle des exportations et peuvent etre soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucleaires, des missiles, des armes biologiques et chimiques ou du nucleaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou reexportations vers des pays sous embargo des Etats-Unis, ou vers des entites figurant sur les listes d'exclusion d'exportation americaines, y compris, mais de maniere non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une facon directe ou indirecte, aux exportations des produits ou des services qui sont regi par la legislation americaine en matiere de controle des exportations et la liste de ressortissants specifiquement designes, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Preface vii

1. ILOM Overview 1

What Is ILOM? 2

What Does ILOM Do? 2

ILOM Features and Functionality 4

New Features in ILOM 3.0 5

Roles for ILOM User Accounts 6

ILOM 3.0 User Account Roles 6

Support for ILOM 2.x User Accounts 8

ILOM Interfaces 8

ILOM on the Server and CMM 9

Initial Login to ILOM 10

`root` and `default` User Accounts 10

`root` User Account 10

`default` User Account 11

Inventory and Component Management 11

2. ILOM Network Configurations 13

ILOM Network Management 14

ILOM Connection Methods 14
Initial Setup Worksheet 15
Network Port Assignments 16
ILOM Communication Settings 17

3. User Account Management 19

Guidelines for Managing User Accounts 20
User Account Roles and Privileges 21
Single Sign On 22
SSH Host Key-Based Authentication 22
Active Directory 23
User Authentication and Authorization 23
User Authorization Levels 23
Lightweight Directory Access Protocol 24
LDAP/SSL 25
RADIUS 25

4. System Monitoring and Alert Management 27

System Monitoring 28
Sensor Readings 28
System Indicators 29
Fault Management 30
ILOM Event Log 31
Syslog Information 32
Collect SP Data to Diagnose System Problems 32
Alert Management 33
Alert Rule Configuration 33
Alert Rule Property Definitions 34
Alert Management From the CLI 36

Alert Management From the Web Interface 37
Alert Management From an SNMP Host 38

5. Power Monitoring and Management Interfaces 39

Power Monitoring Interfaces 40
Power Monitoring Terminology 40
Power Policy 41

6. Configuration Management and Firmware Updates 43

Configuration Management Tasks 44
Backup and Restore Operations 45
Reset to Defaults Feature 46
ILOM Firmware Updates 47
Identification of ILOM Version Information 47
Process for Updating the Firmware 48
Preserve Configuration Option 48
Troubleshoot an Update Session If Network Failure Occurs 49

7. Remote Host Management Options 51

Remote Management Options 52
Power Control 52
ILOM CLI – Remote Power Commands 53
ILOM Web Interface – Remote Power Controls 53
Diagnostics for x64 or SPARC Systems 54
Storage Redirection CLI 55
First Time Access 55
Storage Redirection CLI Architecture 56
Default Network Communication Port 57
Sun ILOM Remote Console 57
Single or Multiple Remote Host Server Management Views 58

Installation Requirements 60

Network Communication Ports and Protocols 61

Sign In Authentication Required 61

CD and Diskette Redirection Operation Scenarios 62

A. Example Setup of Dynamic DNS 65

B. Glossary 71

Index 91

Preface

Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide describes ILOM features that are common to Sun rackmounted servers or server modules (blade servers) that support ILOM. You can access these ILOM features and perform ILOM tasks using different user interfaces, regardless of the Sun server platform that ILOM is managing.

Related Documentation

To fully understand the information that is presented in this guide, use this document in conjunction with the documents listed in the following table. These documents are available online at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

These documents are also available with you platform documentation set at:

http://docs.sun.com/app/docs/prod/servers

First read this ILOM 3.0 Concepts Guide to learn about ILOM's features and functionality. To set up a new system supported by ILOM, refer to the ILOM 3.0 Getting Started Guide, where you will find the procedures for connecting to the network, logging in to ILOM for the first time, and configuring a user account or directory service. Then, decide which ILOM interface you want to use to perform other ILOM tasks. You can now refer to the the appropriate ILOM 3.0 Procedures Guide for your selected interface.

The following table lists the ILOM 3.0 Documentation Collection.

Title	Content	Part Number	Format
Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide	Information that describes ILOM features and functionality	820-6410	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide	Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service	820-5523	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM web interface	820-6411	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM CLI	820-6412	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide	Information and procedures for accessing ILOM functions using SNMP or IPMI management hosts	820-6413	PDF HTML

In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement documents present ILOM features and tasks that are specific to the server platform you are using. Use the ILOM 3.0 Documentation Collection in conjunction with the ILOM Supplement that comes with your server platform.

Documentation, Support and Training

Sun Function	URL
Documentation	http://docs.sun.com
Support	http://www.sun.com/support/
Training	http://www.sun.com/training/

ILOM 3.0 Version Numbers

ILOM 3.0 has implemented a new version numbering scheme to help you identify which version of ILOM you are running on your system. The numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of ILOM.
- `b` – Represents a minor version of ILOM.
- `c` – Represents the update version of ILOM.
- `d` – Represents a micro version of ILOM. Micro versions are managed per platform or group of platforms. See your platform Product Notes for details.
- `e` – Represents a nano version of ILOM. Nano versions are incremental iterations of a micro version.

For example, ILOM 3.1.2.1.a would designate:

- ILOM 3 as the major version of ILOM
- ILOM 3.1 as a minor version of ILOM 3
- ILOM 3.1.2 as the second update version of ILOM 3.1
- ILOM 3.1.2.1 as a micro version of ILOM 3.1.2
- ILOM 3.1.2.1.a as a nano version of ILOM 3.1.2.1

Product Identity Information

Product identity information enables a system to register itself and use certain automated services based on the service contract associated with its identity. You can use product identity information to uniquely identify a system. You also need to supply the product identity information to Sun when you request service for the system. Product identity consists of the following information:

- `product_name`: Name under which a product is sold. For example, "SUN FIRE X4100 M2."
- `product_part_number`: Namespace assigned by manufacturing within which the product serial number is unique. A product part number never maps to more than one product. For example, "602-3098-01."
- `product_serial_number`: Unique identity assigned to each instance of a product by manufacturing. For example, "0615AM0654A."
- `product_manufacturer`: Manufacturer of the product. For example, 'SUN MICROSYSTEMS."

TABLE P-1 describes the common product identity information used by ILOM.

TABLE P-1 Common Product Identity Information

Required Interface	Target	Minimal Properties
Basic product information on server (rackmounted and blade)	/SYS	product_name product_part_number product_serial_number product_manufacturer
Basic product information on chassis monitoring module (CMM)	/CH	product_name product_part_number product_serial_number product_manufacturer
Basic chassis information on blade	/SYS/MIDPLANE	product_name product_part_number product_serial_number product_manufacturer
Location of blade within the chassis	/SYS/SLOTID	type class value
Location of chassis within a rack	/CH	rack_location

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

http://www.sun.com/hwdocs/feedback

Please include the title and part number of your document with your feedback:

Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide, part number 820-6410-10.

CHAPTER 1

ILOM Overview

Topics

Description	Links
Learn about ILOM features and functionality	• "What Is ILOM?" on page 2 • "What Does ILOM Do?" on page 2 • "ILOM Features and Functionality" on page 4 • "New Features in ILOM 3.0" on page 5 • "Roles for ILOM User Accounts" on page 6 • "ILOM Interfaces" on page 8 • "ILOM on the Server and CMM" on page 9 • "Initial Login to ILOM" on page 10 • "`root` and `default` User Accounts" on page 10 • "Inventory and Component Management" on page 11

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• CLI Overview	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Web Interface Overview	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• SNMP and IPMI hosts	• SNMP Overview • IPMI Overview	*Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

What Is ILOM?

Sun's Integrated Lights Out Manager (ILOM) provides advanced service processor hardware and software that you can use to manage and monitor your Sun servers. ILOM's dedicated hardware and software is preinstalled on a variety of Sun server platforms, including x64-based Sun Fire™ servers, Sun Blade™ modular chassis systems, Sun Blade server modules, as well as on SPARC-based servers. ILOM is a vital management tool in the data center and can be used to integrate with other data center management tools already installed on your systems.

Sun is currently transitioning many systems to support ILOM so that customers will have a single, consistent, and standards-based service processor (SP) across Sun's product lines. For customers, this means you will have:

- Single, consistent system management interfaces for operators
- Rich protocol and standards support
- Broadening third-party management support
- System management functions integrated into Sun servers at no extra cost

What Does ILOM Do?

ILOM enables you to actively manage and monitor the server independently of the operating system state, providing you with a reliable Lights Out Management (LOM) system. With ILOM, you can proactively:

- Learn about hardware errors and faults as they occur
- Remotely control the power state of your server
- View the graphical and non-graphical consoles for the host
- View the current status of sensors and indicators on the system
- Determine the hardware configuration of your system
- Receive generated alerts about system events in advance via IPMI PETs, SNMP Traps, or Email Alerts.

The ILOM service processor (SP) runs its own embedded operating system and has a dedicated Ethernet port, which together provide out-of-band management capability. In addition, you can access ILOM from the server's host operating system that Sun supports (Solaris, Linux, and Windows). Using ILOM, you can remotely manage your server as if you were using a locally attached keyboard, monitor, and mouse.

ILOM automatically initializes as soon as power is applied to your server. It provides a full-featured, browser-based web interface and has an equivalent command-line interface (CLI). There is also an industry-standard SNMP interface and IPMI interface.

You can easily integrate these management interfaces with other management tools and processes that you might have working already with your servers, such as Sun™ xVM Ops Center. This easy-to-use system management platform for Solaris and Linux provides the tools that you need to efficiently manage systems on your network. Sun xVM Ops Center can discover new and existing systems on your network, update firmware and BIOS configurations, provision the operating environment with off-the-shelf distributions or Solaris images, manage updates and configuration changes, and remotely control key aspects of the service processor such as boot control, power status, and indicator lights. For more information about Sun xVM Ops Center, go to:

http://www.sun.com/software/products/xvmopscenter/index.jsp

In addition, you can integrate ILOM with these third-party management tools:

- Altiris Deployment Solution
- BMC PATROL Enterprise Manager
- CA Unicenter Network and Systems Management (NSM)
- HP OpenView Operations for UNIX
- HP OpenView Operations for Windows
- HP Systems Insight Manager
- IBM Director
- IBM Tivoli Enterprise Console
- IBM Tivoli Monitoring (ITM)
- IBM Tivoli Netcool/OMNIbus
- IPMItool 1.8.8 for Microsoft Windows 2003
- Microsoft Operations Manager
- Microsoft System Management
- Microsoft Systems Center Operations Manager
- Sun IPMI System Management Driver
- Sun ILOM PET Events MIB
- Service Processor Error Injector

A description of these third-party system management tools and their support for Sun systems is available at:

http://www.sun.com/system-management/tools.jsp

ILOM Features and Functionality

Whether you are using ILOM 2.x or ILOM 3.x firmware, ILOM offers a full set of features, functions, and protocols that will help you monitor and manage your server systems.

TABLE 1-1 ILOM Features and Functionality

ILOM Feature	What You Can Do
Dedicated service processor and resources	• Manage the server without consuming system resources • Continue to manage the server using standby power even when the server is powered-off
Simple ILOM initial configuration	• Manual SP configuration, including IP address, through BIOS interface, serial or Ethernet SP ports, or host OS
Downloadable firmware updates	• Download firmware updates via browser-based web interface
Remote hardware monitoring	• Monitor system status and event logs • Monitor customer-replaceable units (CRUs) and field-replaceable units (FRUs), including power supplies, fans, disks, CPUs, memory, and motherboard • Monitor environmentals (component temperatures) • Monitor sensors, including voltage and power • Monitor indicators (LEDs)
Hardware and FRU inventory and presence	• Identify installed CRUs and FRUs and their status • Identify part numbers, versions, and product serial numbers • Identify NIC card MAC addresses
Remote Access	• Redirect the system serial console via serial port and LAN • Access keyboard, video, and mouse (KVM) on remote x64 systems and on some SPARC systems • Redirect the OS graphical console to a remote client browser • Connect a remote CD/DVD/floppy to the system for remote storage
System power control and monitoring	• Power the system on or off, either locally or remotely • Force power-off for emergency shutdown or perform a graceful shutdown to shut down the host operating system before power off

TABLE 1-1 ILOM Features and Functionality *(Continued)*

ILOM Feature	What You Can Do
Configuration and management of user accounts	• Configure local user accounts • Authenticate user accounts using LDAP, LDAP/SSL, RADIUS, and Active Directory
Error and fault management	• Monitor system BIOS, POST, and sensor messages • Log events in a consistent method for all "service" data • Monitor hardware and system-related errors, as well as ECC memory errors, reported into SP logs, syslog, and remote log-host
System alerts, including SNMP traps, IPMI PETs, remote syslog, and email alerts	• Monitor components using industry-standard SNMP commands and the IPMItool utility.

New Features in ILOM 3.0

ILOM 3.0 is enhanced with many new features and functions that were not available in ILOM 2.x, including improved security, improved usability, and easier integration into your data center environment. TABLE 1-2 lists new features for ILOM 3.0.

TABLE 1-2 ILOM 3.0 New Features

Category	Feature
General Functionality	
	DNS support
	Timezone support
	Configuration backup and restore
	Restore to factory defaults
	Enhanced LDAP and LDAP/SSL support
	Java-based remote storage CLI
	Power management capabilities
	Ability to generate new SSH keys
Scalability and Usability	
	User-configurable filtering of hardware monitoring information in CLI and web interface
	Use host name to access other services by name, such as LDAP, Active Directory, LDAP/SSL

TABLE 1-2 ILOM 3.0 New Features *(Continued)*

Category	Feature
Security	
	More granular user roles
	Predefined `root` and `default` accounts
	User SSH key authentication
	Ability to disable the network management port when you are using only the serial port
	Ability to disable individual services, such as IPMI, SSH, and KVMS, so that the port is closed
Serviceability	
	Data collection utility to diagnose system problems

Roles for ILOM User Accounts

For ILOM 3.0, user roles are implemented to control user privileges. However, for backward compatibility, ILOM 2.x style user accounts (which have either Administrator or Operator privileges) are still supported.

ILOM 3.0 User Account Roles

For ILOM 3.0, user accounts have defined roles that determine ILOM user access and privileges. TABLE 1-3 describes the roles that you can assign to ILOM 3.0 user accounts.

TABLE 1-3 ILOM 3.0 User Account Roles

Roles	Definition	Privileges
a	Admin	A user who is assigned the Admin (a) role is authorized to view and change the state of ILOM configuration variables. With the exception of tasks that users who have User Management, Console, and Reset and Host Control roles, users assigned the Admin role are authorized to perform all other ILOM functions.
u	User Management	A user who is assigned the User Management (u) role is authorized to create and delete user accounts, change user passwords, change roles assigned to other users, and enable/disable the physical-access requirement for the default user account. This role also includes authorization to set up LDAP, LDAP/SSL, RADIUS, and Active Directory.
c	Console	A user who is assigned the Console (c) role is authorized to access the ILOM Remote Console and the SP console and to view and change the state of the ILOM console configuration variables.
r	Reset and Host Control	A user who is assigned the Reset and Host Control (r) role is authorized to operate the system, which includes power control, reset, hot-plug, enabling and disabling components, and fault management. This role maps very closely to the ILOM 2.0 user with Operator privileges.
o	Read Only	A user who is assigned the Read Only (o) role is authorized to view the state of the ILOM configuration variables but cannot make any changes. Users assigned this role can also change the password and the Session Time-Out setting for their own user account.
s	Service	A user who is assigned the Service (s) role can assist Sun service engineers in the event that on-site service is required.

Support for ILOM 2.x User Accounts

For backward compatibility, ILOM 3.0 supports ILOM 2.x user accounts such that users with ILOM 2.x Administrator or Operator privileges are granted ILOM 3.0 roles that match those privileges. TABLE 1-4 lists the roles assigned to users with Administrator and Operator privileges.

TABLE 1-4 ILOM 3.0 Roles Granted to ILOM 2.x User Accounts

2.x User Privileges	ILOM 3.0 User Roles Granted
Administrator	Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o)
Operator	Console (c), Reset and Host Control (r), and Read Only (o) **Note -** To make the level of authorization granted to users with Operator privileges consistent with 2.x capabilities, the Console (c) role granted in this case is modified to prohibit the user from accessing the ILOM Remote Console (JavaRConsole).

ILOM Interfaces

To access all of ILOM's features and functions, you can choose to use a browser-based web interface, a command-line interface, or industry-standard protocols. For more information on ILOM interfaces, see the Overview chapters in the ILOM 3.0 Procedures Guides.

ILOM supports multiple interfaces for accessing its features and functions. You can choose to use a browser-based web interface, a command-line interface, or industry-standard protocols.

- **Web interface** – The web interface provides an easy-to-use browser interface that enables you to log in to the SP, then to perform system management, monitoring, and IPMI tasks.
- **Command-line interface (CLI)** – The command-line interface enables you to operate ILOM using keyboard commands and adheres to industry-standard DMTF-style CLI and scripting protocols. ILOM supports SSH v2.0 and v3.0 for secure access to the CLI. Using the CLI, you can reuse existing scripts with Sun systems, and automate tasks using familiar interfaces.
- **Remote Console** – The ILOM Remote Console (JavaRConsole) enables you to access your x64 or SPARC server's console remotely. It redirects the keyboard, mouse, and video screen, and can redirect input and output from the local machine's CD and diskette drives.

- **Intelligent Platform Management Interface (IPMI)** – Using IPMI v1.5 or v2.0 and the IPMItool utility, you can manage and configure devices using a CLI to retrieve information from the system's baseboard management controller (BMC). With IPMItool, you can monitor the status of hardware components remotely, monitor system logs, receive reports about replaceable components, and redirect the server console.
- **Simple Network Management Protocol (SNMP) interface** – ILOM also provides an SNMP v3.0 interface for third-party applications such as HP OpenView and IBM Tivoli. Some of the MIBs supported by ILOM 3.0 include:
  - SUN-PLATFORM-MIB
  - SUN-ILOM-CONTROL-MIB
  - SUN-HW-TRAP-MIB
  - SUN-ILOM-PET-MIB
  - SNMP-FRAMEWORK-MIB (9RFC2271.txt)
  - SNMP-MPD-MIB (RFC2572)
  - System and SNMP groups from SNMPv2-MIB (RFC1907)
  - entPhysicalTable from ENTITY-MIB (RFC2737)

For a complete list of SNMP MIBs supported and used by ILOM, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide.*

ILOM on the Server and CMM

ILOM supports two ways of managing a system: using the SP directly or using the chassis monitoring module (CMM), if you are using a modular chassis system.

- **Using the service processor directly** – Communicating directly with the rackmounted server SP or server module SP enables you to manage individual server operations. This approach might be useful when troubleshooting a server module or rackmounted server, or controlling access to specific servers in your data center.
- **Using the chassis monitoring module** – If you are using a modular chassis system, managing the system from the CMM enables you to use ILOM to set up and manage components throughout the entire modular chassis system, or to drill down to manage an individual server module.

Initial Login to ILOM

You can log in to ILOM 3.0 for the first time using the `root` user account. This `root` user account will be familiar to users who are migrating from ILOM 2.x to ILOM 3.0.

For more information and procedures for logging in to and out of ILOM, see:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

`root` and `default` User Accounts

ILOM 3.0 provides two preconfigured accounts: the `root` user account and the `default` user account. You will use the `root` account for initial login to ILOM. This `root` user account will be familiar to users who are migrating from ILOM 2.x to ILOM 3.0 and who know how to log in using the `root` user account. The `default` user account is a new feature in ILOM 3.0 that is used for password recovery.

`root` User Account

The `root` user account is persistent and is available on all interfaces (web interface, CLI, SSH, serial console, and IPMI) unless you choose to delete the `root` account. The `root` account provides built-in administrative privileges (read and write) for all ILOM features, functions, and commands.

To log in to ILOM, use the following `root` account user name and password:

User name: **`root`**

Password: **`changeme`**

To prevent unauthorized access to your system, you should change the `root` password (`changeme`) on each service processor (SP) or chassis monitoring module (CMM) installed in your system. Alternatively, you can delete the `root` account to secure access to your system. However, before you delete the `root` account, you must set up a new user account or configure a directory service so that you will be able to log in to ILOM.

`default` User Account

The `default` user account is used for password recovery. The `default` user account is available through the serial console only and you must prove physical presence at the server to use the `default` user account. The `default` user account cannot be changed or deleted.

If you delete the `root` account before you have configured another user account to log in to ILOM, you can use the `default` account as an alternative way to to log in and re-create the `root` account. To re-create the `root` user account, use the normal ILOM user commands to create a new account. For information about how to create a user account, see "Add User Account and Assign Privileges" in either the web interface or CLI section of the *Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.

For password recovery, use the following user name and password to log in using the `default` account:

User name: **`default`**

Password: **`defaultpassword`**

Inventory and Component Management

With ILOM, you can view component details such as the component name, type, and fault status. In addition, you can use ILOM to prepare to remove and install components and to enable and disable components. To learn how to perform these tasks, refer to the ILOM 3.0 Procedures Guides.

CHAPTER 2

ILOM Network Configurations

Topics

Description	Links
Learn about ILOM network management and connection methods	• "ILOM Network Management" on page 14
Learn about ILOM network communication settings and network port assignments	• "ILOM Communication Settings" on page 17 • "Network Port Assignments" on page 16

Related Topics

For ILOM	Chapter or Section	Guide
• Getting started	• Connecting to ILOM • Initial ILOM Setup Procedures Using the Web Interface • Initial ILOM Setup Procedures Using the CLI	*Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523-10)
• CLI	• Logging In to and Out of ILOM • Configuring Communication Settings • Example Setup of Dynamic DNS	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Logging In to and Out of ILOM • Configuring Communication Settings	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Configuring ILOM Communication Settings	*Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

ILOM Network Management

You can establish communication with ILOM through a console connection to the serial management port on the server or chassis monitoring module (CMM), or through an Ethernet connection to the network management port on the server or CMM.

A dedicated network management port will help you manage your server platform optimally with ILOM. Using the network management port, traffic destined for ILOM is kept separate from any data transfers made by the host operating system.

Refer to your platform documentation to determine how to connect to your network management port.

You can use Dynamic DNS to automatically assign a host name and IP address on new ILOM installations based on the system's serial number. See Appendix A for an overview of Dynamic DNS and configuration instructions.

ILOM Connection Methods

The way in which you connect to ILOM depends on your server platform.

The following table lists the different methods you can use to connect to ILOM.

TABLE 2-1 ILOM Connection Methods

Connection Method	Rack-Mounted	Blade	Supported Interface	Description
Ethernet network management connection	Yes	Yes	CLI and web interface	Connect to the Ethernet network management port. You must know ILOM's host name or IP address.
Serial connection	No	Yes	CLI only	Connect directly to the serial management port. Refer to your platform documentation for details.

Note – ILOM supports a maximum of 10 active sessions, including serial, Secure Shell (SSH), and web interface sessions.

Initial Setup Worksheet

The worksheet in TABLE 2-2 describes the information that you need to establish initial communication with ILOM

TABLE 2-2 Initial Setup Worksheet to Establish Communication With ILOM

Information for Setup	Requirement	Description
Management Connection–Serial	Optional - *if using DHCP for network configuration* Mandatory - *if the network configuration is static, or if you are not using a network*	If you are not using a DHCP server to configure the network to the SP or CMM, you must establish a local serial console connection to ILOM via the serial management port on the server or CMM. If you are not using a network, or you are not using DHCP to configure your network, you must establish a local serial console connection to ILOM via the serial management port on the server or CMM. For more information about how to attach a serial console to a server or CMM, refer to your platform documentation.
Management Connection–Ethernet	Optional	Connect your local area network to the Ethernet network management port of a server or CMM. Refer to your platform documentation for instructions on how to connect. Decide whether to obtain network setting configuration using DHCP or to configure static network settings.
SP Host Name Assignment	Optional	You can assign a meaningful host name to a server SP. For more information, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.
System Identifier Assignment	Optional	You can assign a system identifier (meaningful name) to a Sun server. For more information, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* or the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.
Dynamic DNS Configuration	Optional	You can configure Dynamic DNS to support the use of host names to access server SPs. See the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* for Dynamic DNS configuration procedures.

Network Port Assignments

TABLE 2-3 identifies the default network ports used by ILOM. Most of these network ports are configurable.

TABLE 2-3 ILOM Network Ports

Port	Protocol	Application
Common Network Ports		
80	HTTP over TCP	Web (user-configurable)
443	HTTPS over TCP	Web (user-configurable))
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (outgoing)
123	NTP over UDP	NTP - Network Time Protocol (outgoing)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (user-configurable)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (outgoing; user-configurable)
514	Syslog over UDP	Syslog - (outgoing)
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service (outgoing; user-configurable)
SP Network Ports		
5120	TCP	ILOM Remote Console: CD
5123	TCP	ILOM Remote Console: Diskette
5121	TCP	ILOM Remote Console: Keyboard and Mouse
7578	TCP	ILOM Remote Console: Video
CMM Network Ports		
8000 - 8023	HTTP over TCP	ILOM drill-down (blades)
8400 - 8423	HTTPS over TCP	ILOM drill-down (blades)
8200 - 8219	HTTP over TCP	ILOM drill-own (NEMs)
8600 - 8619	HTTPS over TCP	ILOM drill-down (NEMs)

ILOM Communication Settings

You can use the ILOM CLI interface, web interface, or SNMP to manage ILOM's communication settings, including network, serial port, web, and Secure Shell (SSH) configurations. ILOM lets you view and configure system host names, IP addresses, DNS settings, and serial port settings. You also can enable or disable HTTP or HTTPS web access, and enable or disable SSH.

For more information and procedures for managing ILOM communication settings, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

CHAPTER 3

User Account Management

Topics

Description	Links
Learn about managing user accounts and roles	• "Guidelines for Managing User Accounts" on page 20 • "User Account Roles and Privileges" on page 21
Learn about Single Sign On	• "Single Sign On" on page 22
Learn about SSH authentication	• "SSH Host Key-Based Authentication" on page 22
Learn about Active Directory	• "Active Directory" on page 23
Learn about LDAP	• "Lightweight Directory Access Protocol" on page 24 • "LDAP/SSL" on page 25
Learn about RADIUS	• "RADIUS" on page 25

Related Topics

For ILOM	Chapter or Section	Guide
• Getting started	• Initial ILOM Seup Procedures Using the Web Interface • Initial ILOM Setup Procedures Using the CLI	*Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523-10)
• CLI	• Managing User Accounts	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Managing User Accounts	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

Related Topics

For ILOM	Chapter or Section	Guide
• SNMP and IPMI hosts	• Managing User Accounts Using SNMP • SNMP Command Reference	*Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

Guidelines for Managing User Accounts

Apply the following general guidelines when you manage user accounts:

- ILOM supports a maximum of 10 user accounts.
- The user name of an account must be at least eight characters and no more than 16 characters. User names are case sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.
- Each user account is assigned one or more advanced roles, which determine the privileges of the user account. Depending on the roles assigned to your user account, you can use the ILOM web interface, command-line interface (CLI), or SNMP to view account information and perform various administrative functions.
- You can either configure local accounts or you can have ILOM authenticate accounts against a remote user database, such as Active Directory, LDAP, LDAP/SSL, or RADIUS. With remote authentication, you can use a centralized user database rather than configuring local accounts on each ILOM instance.

For more information and procedures for managing user accounts, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

User Account Roles and Privileges

ILOM 3.0 user accounts have defined roles that determine ILOM user access and rights. You can manage user accounts using the ILOM web interface or the CLI. The roles assigned to ILOM accounts are listed in TABLE 3-1.

TABLE 3-1 ILOM 3.0 User Account Roles

Roles	Definition	Privileges
a	Admin	A user who is assigned the Admin (a) role is authorized to view and change the state of ILOM configuration variables. With the exception of tasks that users who have User Management, Console, and Reset and Host Control roles, users assigned the Admin role are authorized to perform all other ILOM functions.
u	User Management	A user who is assigned the User Management (u) role is authorized to create and delete user accounts, change user passwords, change roles assigned to other users, and enable/disable the physical-access requirement for the default user account. This role also includes authorization to set up LDAP, LDAP/SSL, RADIUS, and Active Directory.
c	Console	A user who is assigned the Console (c) role is authorized to access the ILOM Remote Console and the SP console and to view and change the state of the ILOM console configuration variables.
r	Reset and Host Control	A user who is assigned the Reset and Host Control (r) role is authorized to operate the system, which includes power control, reset, hot-plug, enabling and disabling components, and fault management. This role maps very closely to the ILOM 2.0 user with Operator privileges.
o	Read Only	A user who is assigned the Read Only (o) role is authorized to view the state of the ILOM configuration variables but cannot make any changes. Users assigned this role can also change the password and the Session Time-Out setting for their own user account.
s	Service	A user who is assigned the Service (s) role can assist Sun service engineers in the event that on-site service is required.

Single Sign On

Single Sign On (SSO) is a convenient authentication service that enables you to log in to ILOM once to establish your credentials, thus reducing the number of times you need to enter your password to gain access to ILOM. Single Sign On is enabled by default. As with any authentication service, authentication credentials are passed over the network. If this is not desirable, consider disabling the SSO authentication service.

SSH Host Key-Based Authentication

Traditionally, automation of password authentication is made possible by SSH key-based authentication. Prior to the implementation of the SSH key-based authentication feature, users that logged in to the ILOM SP using SSH were required to supply a password interactively. An automatic mechanism for password authentication is most beneficial when you have a large number of systems that require a similar update.

The primary capabilities afforded by SSH key-based authentication are as follows:

- Users are able to write scripts that automatically copy log files off of a service processor (SP) for archival and analysis.
- Users are able to write scripts that automatically and/or regularly execute SP commands over a network-based SSH connection from a remote system.

Thus, SSH key-based authentication enables you to accomplish both of the above activities through the use of scripts that execute without human intervention and that do not include embedded passwords.

Regarding the use and handling of SSH keys, ILOM enables users to add generated keys to individual user accounts on the SP.

For more information and procedures for adding and deleting SSH keys, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Active Directory

ILOM supports Active Directory, the distributed directory service included with Microsoft Windows Server operating systems. Like an LDAP directory service implementation, Active Directory is used to authenticate user credentials.

Note – The service processor (SP) expects to communicate with the Active Directory server using a secure channel. To ensure security, the Active Directory server should be loaded with a certificate that can be presented during the SP user authentication process so that protocol negotiations can allow a private channel to be set up.

User Authentication and Authorization

Active Directory provides both authentication of user credentials and authorization of user access levels to networked resources. Active Directory uses authentication to verify the identity of a user before that user can access system resources. Active Directory uses authorization to grant specific access privileges to a user in order to control a user's rights to access networked resources. User access levels are configured or learned from the server based on the user's group membership in a network domain, which is a group of hosts identified by a specific Internet name. A user can belong to more than one group. Active Directory authenticates users in the order in which the user's domains were configured.

User Authorization Levels

Once authenticated, the user's authorization level can be determined in the following ways:

- In the simplest case, the user authorization of either Operator, Administrator, or Advanced Roles (see "User Account Roles and Privileges" on page 21) is learned directly through the Active Directory's configuration of the SP. Access and authorization levels are dictated by the `defaultrole` property. Setting up users in the Active Directory database requires only a password with no regard to group membership. On the SP, the `defaultrole` will be set to either Administrator, Operator, or the Advanced Role settings `a/u/c/r/o/s`. All users authenticated through Active Directory are assigned the privileges associated with the Administrator, Operator, or Advanced Roles based solely on this configuration.

- A more integrated approach is also available by querying the server. For configuration, the SP Administrator Group Tables, Operator Group Tables, or Custom Group Tables must be configured with the corresponding group names from the Active Directory server that will be used to determine access levels. Up to five Active Directory groups can be entered to designate an Administrator; another five can be used to assign Operator privileges; and up to five groups can be assigned to Custom Groups, which contain Advanced Roles (see "User Account Roles and Privileges" on page 21). Group membership of the user is used to identify the proper access level of either Administrator, Operator, or Advanced Roles by looking up each group name in the configured Active Directory tables on the SP. If the user's group list is not in either of the defined SP user groups, then access is denied. A user assigned to more than one group will receive the sum of all privileges.

For more information and procedures for configuring Active Directory settings, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

Lightweight Directory Access Protocol

ILOM supports Lightweight Directory Access Protocol (LDAP) authentication for users, based on the OpenLDAP software. LDAP is a general-purpose directory service. A directory service is a centralized database for distributed applications designed to manage the entries in a directory. Thus, multiple applications can share a single user database. For more detailed information about LDAP, go to:

`http://www.openldap.org/`

For more information and procedures for configuring LDAP settings, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

LDAP/SSL

LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. To configure LDAP/SSL in a SP, you need to enter basic data—such as primary server, port number, and certificate mode—and optional data such as alternate server or event or severity levels. You can enter this data using the LDAP/SSL configuration page of the ILOM web interface, the CLI, or SNMP.

For more information and procedures for configuring LDAP/SSL settings, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

RADIUS

ILOM supports Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS is an authentication protocol that facilitates centralized user administration. RADIUS provides many servers shared access to user data in a central database, providing better security and easier administration. A RADIUS server can work in conjunction with multiple RADIUS servers and other types of authentication servers.

RADIUS is based on a client-server model. The RADIUS server provides the user authentication data and can grant or deny access, and the clients send user data to the server and receive an “accept” or “deny” response. In the RADIUS client-server model, the client sends an Access-Request query to the RADIUS server. When the server receives an Access-Request message from a client, it searches the database for that user's authentication information. If the user's information is not found, the server sends an Access-Reject message and the user is denied access to the requested service. If the user's information is found, the server responds with an Access-Accept message. The Access-Accept message confirms the user's authentication data and grants the user access to the requested service.

All transactions between the RADIUS client and server are authenticated by the use of a specific text string password known as a shared secret. The client and server must each know the shared secret because it is never passed over the network. You must know the shared secret to configure RADIUS authentication for ILOM.

In order to use RADIUS authentication with ILOM, you must configure ILOM as a RADIUS client.

For more information and procedures for configuring RADIUS settings, see one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

CHAPTER 4

System Monitoring and Alert Management

Topics

Description	Links
Learn about system monitoring features in ILOM	• "System Monitoring" on page 28 • "Sensor Readings" on page 28 • "System Indicators" on page 29 • "Fault Management" on page 30 • "ILOM Event Log" on page 31 • "Syslog Information" on page 32 • "Collect SP Data to Diagnose System Problems" on page 32
Learn about managing system alerts in ILOM	• "Alert Management" on page 33 • "Alert Management From the CLI" on page 36 • "Alert Management From the Web Interface" on page 37 • "Alert Management From an SNMP Host" on page 38

Related Topics

For ILOM	Section	Guide
• CLI	• Monitoring System Components • Managing System Alerts	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Monitoring System Components • Managing System Alerts	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

Related Topics

For ILOM	Section	Guide
• IPMI and SNMP hosts	• Monitoring System Components • Managing System Alerts	*Sun Integrated Lights Out Manager (ILOM) 3.0 IPMI and SNMP Procedures Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

System Monitoring

The system monitoring features in ILOM enable you to easily determine the health of the system and to detect errors, at a glance, when they occur. For instance, in ILOM you can:

- View instantaneous sensor readings about system component temperatures, current, voltage, speed, and presence. For more information, see "Sensor Readings" on page 28.
- Determine the state of indicators throughout the system. For more information, see "System Indicators" on page 29.
- Identify system errors and view event information in the ILOM event log. For more information, see "ILOM Event Log" on page 31.
- Combine and view events from multiple instances in ILOM by sending Syslog information. For more information, see "Syslog Information" on page 32.
- Collect data for use by Sun Services personnel to diagnose system problems. For more information, see "Collect SP Data to Diagnose System Problems" on page 32.

Sensor Readings

All Sun server platforms are equipped with a number of sensors that measure voltages, temperatures, fan speeds, and other attributes about the system. Each sensor in ILOM contains nine properties describing various settings related to a sensor such as sensor type, sensor class, sensor value, as well as the sensor values for upper and lower thresholds.

ILOM regularly polls the sensors in the system and reports any events it encounters about sensor state changes or sensor threshold crossings to the ILOM event log. Additionally, if an alert rule was enabled in the system that matched the crossing threshold level, ILOM would automatically generate an alert message to the alert destination that you have defined.

You can view sensor readings from the ILOM web interface or CLI. For details, see "View Sensor Readings" in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

System Indicators

System indicator LEDs are generally illuminated on the system by ILOM based on the Sun server platform policy. Typically the system indicator LEDs are illuminated by ILOM when any of the following conditions occur:

- Fault or error is detected on a component.
- Field-replacement unit (FRU) requires service.
- Hot-plug module is ready for removal.
- Activity is occurring on FRU or system.

You can view the states of system indictors from the ILOM web interface or the CLI. Additionally, in some instances, you might be able to modify the state of a system indicator. For details, see "View and Manage System Indicators" in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Supported System Indicator States

ILOM supports the following system indicator states:

- **Off** – Normal operating status. Service is not required.
- **Steady On** – Component is ready for removal.
- **Slow Blink** – Component is changing state.
- **Fast Blink** – Helps locate a system in a data center.
- **Standby Blink** – Component is ready for activation, but is not operational at this time.

Types of System Indicator States

ILOM supports two types of system indicator states: *Customer Changeable* and *System Assigned*.

- **Customer Changeable States** – Some system indicator LEDs in ILOM offer customer changeable states. Typically, these types of system indicators provide operational states of various system components. The type of states presented is determined by the system indicator. For example, depending on the system indicator, the following customer changeable states might be present:
  - **Off** – Normal operating status. Service is not required.
  - **Fast Blink** – Helps locate system in a data center.
- **System Assigned States** – System assigned indicators are *not* customer configurable. These types of system indicators provide read-only values about the operational state of a component. On most Sun server platforms, system assigned indicators are *Service Action Required LEDs*. These types of LEDs are typically illuminated when any of the following conditions are detected:
  - Fault or error is detected on a system component.
  - Hot-plug module is ready for removal.
  - Field-replacement unit (FRU) requires service.

Fault Management

Most Sun server platforms include the fault management software feature in ILOM. This feature enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. In addition to monitoring the system hardware, the fault management software monitors environmental conditions and reports when the system's environment is outside acceptable parameters. Various sensors on the system components are continuously monitored. When a problem is detected, the fault management software automatically:

- Illuminates the Server Action Required LED on the faulted component.
- Updates the ILOM management interfaces to reflect the fault condition.
- Records information about the fault in the ILOM event log.

The type of system components and environmental conditions monitored by the fault management software are determined by the Sun server platform. For more details about which components are monitored by the fault management software, consult your Sun server platform documentation.

Note – The ILOM fault management feature is currently available on all Sun server platforms, with the exception of the Sun Fire X4100 or X4200 series servers.

You can view the status of faulted components from the ILOM web interface or CLI. For details, see "View Fault Status" in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

ILOM Event Log

The ILOM event log enables you to view information about any event that occurred on the system. Some of these events include ILOM configuration changes, software events, warnings, alerts, component failure, as well as IPMI events. The type of events recorded in the ILOM event log is determined by the Sun server platform. For information about which events are recorded in the ILOM event log, consult your Sun server platform documentation.

Event Log Time Stamps and ILOM Clock Settings

ILOM captures time stamps in the event log based on the host server UTC/GMT timezone. However, if you view the event log from a client system that is located in a different timezone, the time stamps are automatically adjusted to the timezone of the client system. Therefore, a single event in the ILOM event log might appear with two timestamps.

In ILOM, you can choose to manually configure the ILOM clock based on the UTC/GMT timezone of the host server, or you can choose to synchronize the ILOM clock with other systems on your network by configuring the ILOM clock with an NTP server IP address.

Manage Event Log and Time Stamps From CLI, Web, or SNMP Host

You can view and manage the event log and time stamps in ILOM from the CLI, web interface, or an SNMP host. For details, see "Configure Clock Settings" and "Filter Event Log Output" in the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Syslog Information

Syslog is a standard logging utility used in many environments. Syslog defines a common set of features for logging events and also a protocol for transmitting events to a remote log host. You can use syslog to combine events from multiple instances of ILOM within a single place. The log entry contains all the same information that you would see in the local ILOM event log, including class, type, severity, and description.

For information about configuring ILOM to send syslog to one or two IP addresses, see "Configure Remote Syslog Receiver IP Addresses" in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

Collect SP Data to Diagnose System Problems

The ILOM Service Snapshot utility enables you to produce a snapshot of the SP at any instant in time. You can run the utility from the ILOM CLI or the web interface.

Caution – The purpose of the ILOM Service Snapshot utility is to collect data for use by Sun Services personnel to diagnose system problems. Customers should not run this utility unless requested to do so by Sun Services.

The ILOM Service Snapshot utility gathers service processor (SP) state data. The utility collects log files, runs various commands and collects their output, and sends the data collection as a downloaded file to a user-defined location.

For more information about how to collect SP data to diagnose system problems, see "Collect SP Data to Diagnose System Problems" in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Alert Management

ILOM supports alerts in the form of IPMI PET alerts, SNMP Trap alerts, and Email Notification alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the ILOM SP on your server.

Each Sun server platform is equipped with a number of sensors that measure voltages, temperatures, and other service-related attributes about the system. ILOM automatically polls these sensors and posts any events crossing a threshold to an ILOM event log, as well as generates alert message(s) to one or more customer-specified alert destinations. The alert destination specified must support the receipt of the alert message (IPMI PET or SNMP). If the alert destination does not support the receipt of the alert message, the alert recipient will be unable to decode the alert message.

Caution – ILOM tags all events or actions with LocalTime=GMT (or UTC). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs in ILOM, the event log shows it in UTC, but a client would show it in LocalTime. For more information about ILOM timestamps and clock settings, see "Event Log Time Stamps and ILOM Clock Settings" on page 31.

Alert Rule Configuration

In ILOM you can configure up to 15 alert rules using the ILOM web interface or CLI. For each alert rule you configure in ILOM, you must define three or more properties about the alert depending on the alert type.

The *alert type* defines the messaging format and the method for sending and receiving an alert message. ILOM supports these three alert types:

- IPMI PET alerts
- SNMP Trap alerts
- Email Notification alerts

All Sun server platforms support all three alert types.

Alert Rule Property Definitions

ILOM offers the following property values for defining an alert rule:

- Alert Type
- Alert Level
- Alert Destination
- Alert Destination Port
- Email Custom Sender
- Email Message Prefix
- Email Class Filter
- Email Type Filter
- SNMP Version (*SNMP Trap alerts only*)
- SNMP Community Name or User Name (*SNMP Trap alerts only*)

For information about each of these property values, see TABLE 4-1.

TABLE 4-1 Properties for Defining Alert Rules

Property Name	Requirement	Description
Alert Type	Mandatory	The alert type property specifies the message format and the delivery method that ILOM will use when creating and sending the alert message. You can choose to configure one of the following alert types: • **IPMI PET Alerts**. IPMI Platform Event Trap (PET) alerts are supported on all Sun server platforms and modules, with the exception of a Sun CMM. For each IPMI PET alert you configure in ILOM, you must specify an IP address for an alert destination and one of four supported alert levels. Note that the alert destination specified must support the receipt of IPMI PET messages. If the alert destination does not support the receipt of IPMI PET messages, the alert recipient will not be able to decode the alert message. • **SNMP Trap Alerts**. ILOM supports the generation of SNMP Trap alerts to a customer-specified IP destination. All destinations specified must support the receipt of SNMP Trap messages. Note that SNMP Trap alerts are supported on rackmounted servers and blade server modules. • **Email Notification Alerts**. ILOM supports the generation of Email Notification alerts to a customer-specified email address. To enable the ILOM client to generate Email Notification alerts, ILOM initially requires you to configure the name of the outgoing SMTP email server that would be sending the Email alert messages.

TABLE 4-1 Properties for Defining Alert Rules *(Continued)*

Property Name	Requirement	Description
Alert Destination	Mandatory	The alert destination property specifies where to send the alert message. The alert type determines which destination you can choose to send an alert message. For example, IPMI PET and SNMP Trap alerts must specify an IP address destination. Email Notification alerts must specify an email address. If the proper format is not entered for an alert destination, ILOM will report an error.
Alert Destination Port	Optional	The alert destination port only applies when the alert type is an SNMP Trap. The destination port property specifies the UDP port to which SNMP Trap alerts are sent.
Alert Level	Mandatory	Alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving. Each time you define an alert rule in ILOM, you must specify an alert level. The alert level determines which events generate an alert. The lowest level alert generates alerts for that level and for all alert levels above it. ILOM offers the following alert levels with Minor being the lowest alert offered: • **Minor**. This alert level generates alerts for informational events, lower and upper non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • **Major.** This alert level generates alerts for upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events. • **Critical**. This alert level generates alerts for upper and lower critical events and upper and lower non-recoverable events. • **Down**. This alert level generates alerts for only upper non-recoverable and lower non-recoverable events. • **Disabled**. Disables the alert. ILOM will not generate an alert message. All the alert levels will enable the sending of a alert with the exception of *Disabled*. **Important -** ILOM supports alert level filtering for all IPMI traps and Email Notification traps. ILOM does not support alert level filtering for SNMP traps. To enable the sending of an SNMP trap (but not filter the SNMP trap by alert level) you can choose anyone of the following options: *Minor*, *Major, Critical*, or *Down*. To disable the sending of an SNMP trap, you must choose the *Disabled* option.
Email Custom Sender	Optional	The email custom sender property applies only when the alert type is an email alert. You can use the `email_custom_sender` property to override the format of the "from" address. You can use either one of these substitution strings: <*IPADDRES*S> or <*HOSTNAME*>; for example, alert@[<*IPADDRESS*>]. Once this property is set, this value will override any SMPT custom sender information.

TABLE 4-1 Properties for Defining Alert Rules *(Continued)*

Property Name	Requirement	Description
Email Message Prefix	Optional	The email message prefix property applies only when the alert type is an email alert. You can use the `email_message_prefix` property to prepend information to the message content.
Event Class Filter	Optional	The event class filter property applies only when the alert type is an email alert. The default setting is to send every ILOM event as an email alert. You can use the `event_class_filter` property to filter out all information except the selected event class. You can use "" (empty double quotes) to clear the filter and send information about all classes.
Event Type Filter	Optional	The event type filter property applies only when the alert type is an email alert. You can use the `event_type_filter` property to filter out all information except the event type. You can use "" (empty double quotes) to clear the filter and send information about all event types.
SNMP Version	Optional	The SNMP version property enables you to specify which version of an SNMP trap that you are sending. You can choose to specify: 1, 2c, or 3. This property value only applies to SNMP Trap alerts.
SNMP Community Name or User Name	Optional	The SNMP community name or user name property enables you to specify the community string or SNMP v3 user name used in the SNMP Trap alert. • For SNMP v1 or v2c, you can choose to specify a community name value for an SNMP alert. • For SNMP v3, you can choose to specify a user name value for an SNMP alert. **Note -** If you choose to specify an SNMP v3 user name value, you must define this user in ILOM as an SNMP user. If you do not define this user as an SNMP user, the trap receiver will not be able to decode the SNMP Trap alert. For more information about defining an SNMP user in ILOM, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*, or the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Alert Management From the CLI

You can enable, modify, or disable any alert rule configuration in ILOM from the command-line interface (CLI). All 15 alert rule configurations defined in ILOM are disabled by default. To enable alert rule configurations in ILOM, you must set values for the following properties: alert type, alert level, and alert destination.

You can also generate test alerts to any *enabled* alert rule configuration in ILOM from the CLI. This test alert feature enables you to verify that the alert recipient(s) specified in an *enabled* alert rule configuration receives the alert message.

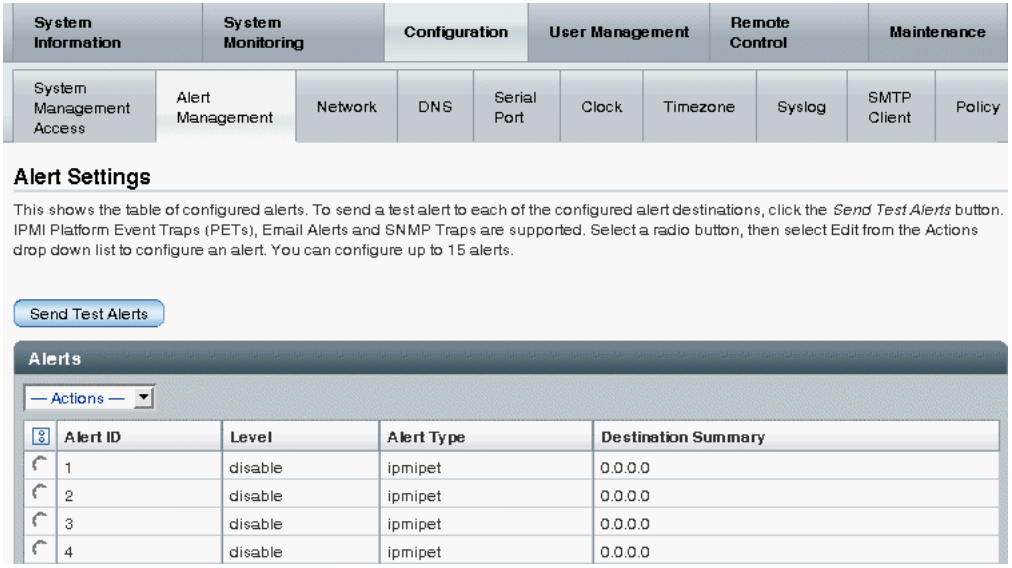
For additional information about how to manage alerts using the ILOM CLI, see "Managing System Alerts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Alert Management From the Web Interface

You can enable, modify, or disable any alert rule configuration in ILOM from the Alert Settings web interface page. All 15 alert rule configurations presented on this page are disabled by default. The Actions drop-down list box on the page enables you to edit the properties associated with an alert rule. To enable an alert rule on this page, you must define an alert type, alert level, and a valid alert destination.

The Alert Settings page also presents a Send Test Alert button. This test alert feature enables you to verify that each alert recipient specified in an enabled alert rule receives an alert message.

FIGURE 4-1 Alert Settings Page


System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
System Management Access
Alert Management
Network
DNS
Serial Port
Clock
Timezone
Syslog
SMTP Client
Policy
Alert Settings
This shows the table of configured alerts. To send a test alert to each of the configured alert destinations, click the Send Test Alerts button. IPMI Platform Event Traps (PETs), Email Alerts and SNMP Traps are supported. Select a radio button, then select Edit from the Actions drop down list to configure an alert. You can configure up to 15 alerts.
Send Test Alerts
Alerts
— Actions —
Alert ID
Level
Alert Type
Destination Summary
1 disable ipmipet 0.0.0.0
2 disable ipmipet 0.0.0.0
3 disable ipmipet 0.0.0.0
4 disable ipmipet 0.0.0.0

For additional information about how to manage alerts using the ILOM web interface, see "Managing System Alerts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

Alert Management From an SNMP Host

You can use the `get` and `set` commands to view and configure alert rule configurations using an SNMP host.

Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information about how to use SNMP to manage system alerts, see "Managing System Alerts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*.

CHAPTER 5

Power Monitoring and Management Interfaces

Topics

Description	Links
Learn about ILOM's power monitoring and power consumption interfaces	• "Power Monitoring Interfaces" on page 40
Become familiar with the terminology and power policy features associated with the power consumption monitoring	• "Power Monitoring Terminology" on page 40 • "Power Policy" on page 41

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Monitoring Power Consumption	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Monitoring Power Consumption	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Monitoring Power Consumption	*Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Power Monitoring Interfaces

Power monitoring interfaces enable real-time power consumption to be monitored. Monitoring in real time means that the service processor (SP) or individual power supply can be polled at any instance to retrieve and report “live” data to within one second accuracy.

Power Monitoring Terminology

Power consumption that is reported includes input and output power. *Input power* is the power that is pulled into the system’s power supplies from an external source. *Output power* is the amount of power provided from the power supply to the system components.

On a rackmount server, the total power consumption is the input power consumed by the server. On a server module (blade), the total power consumption is the input power consumed only by the blade and not including any power consumed by shared components. On a chassis monitoring module (CMM), total power consumption is the input power consumed by the entire chassis or shelf.

You can also monitor hardware configuration maximum power, available power, and permitted power.

Hardware configuration maximum power provides the maximum input power that a system is capable of consuming at any instant given the hardware configuration of the system. Therefore, the hardware configuration maximum power is the sum of the maximum power that each processor, I/O module, memory module, fan, and so forth is capable of consuming.

Note – The hardware configuration maximum power metric is not supported on all systems. Refer to your platform-specific ILOM Supplement or Product Notes for more information.

Available power is the maximum power that the power supplies in the system can draw from an external source. Typically this number is higher than the hardware configuration maximum. The available power for a blade is controlled by the chassis. The chassis guarantees that a certain amount of power will always be available to the blade. If the blade cannot guarantee to stay within the available power provided by the chassis, it will not power on.

Some systems may be able to guarantee a lower maximum consumption than the hardware configuration maximum becuase of software configuration. This guaranteed lower maximum consumption is referred to as *permitted power*. On a rackmount server, permitted power is the maximum input power the server guarantees it will consume at any instant. On a blade, permitted power is the maximum power a blade guarantees it will consume, not including its power load on shared components. On a CMM, permitted power is the maximum input power the entire chassis (all blades, NEMs, fans, and so forth) will consume at any instant. Permitted power will default to the hardware configuration maximum if no software enforced power limit is in effect.

Power Policy

The power policy setting governs system power usage at any point in time. Two power policies are supported: Performance and Elastic.

- **Performance** - The system is allowed to use all of the power that is available.
- **Elastic -** The system power usage is adapted to the current utilization level. For example, the system will power up or down just enough system components to keep relative utilization at 70% at all times, even if workload fluctuates.

Note – The power policy feature is not supported on all platforms. Refer to your platform-specific ILOM Supplement or Product Notes for information about the power policy feature implemented on your platform.

You can access the power monitoring interfaces in ILOM from either the CLI, web interface, IPMI, or SNMP host. For more details about how to use the power monitoring interfaces, see “Monitoring Power Consumption” in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

CHAPTER 6

Configuration Management and Firmware Updates

Topics

Description	Links
Learn about ILOM's configuration management features	• "Configuration Management Tasks" on page 44 • "Backup and Restore Operations" on page 45 • "Reset to Defaults Feature" on page 46
Learn about ILOM's firmware update operations	• "ILOM Firmware Updates" on page 47 • "Identification of ILOM Version Information" on page 47 • "Process for Updating the Firmware" on page 48 • "Preserve Configuration Option" on page 48 • "Troubleshoot an Update Session If Network Failure Occurs" on page 49

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Backing Up and Restoring ILOM Configuration • Updating ILOM Firmware	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Backing Up and Restoring ILOM Configuration • Updating ILOM Firmware	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at:
http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

Configuration Management Tasks

You can perform the following configuration management tasks:

- Back up the ILOM configuration to a XML file on a remote system.
- Use the backup file to restore ILOM to the backed up configuration.
- Use the backup file to install the backed up configuration on other ILOM SPs.
- Reset the ILOM configuration to the default settings.

You can use the Backup and Restore and Reset to Defaults features together in the following ways:

- Save the ILOM configuration to a backup XML file, reset the ILOM configuration to the default settings, and use the command-line interface (CLI) or web interface to create a new ILOM configuration.
- Reset the ILOM configuration to the default settings and restore it using a known good ILOM configuration backup file.
- Use the CLI or web interface to create a new ILOM configuration, save the ILOM configuration to a backup XML file, edit the XML file to remove settings that are unique to a particular system, and perform restore operations to load the backup file to other systems.

Given the above capabilities, the following use cases describe how you might typically use these features:

- You changed your ILOM configuration but it no longer works and you want to recover ILOM by restoring it to a known good configuration. To do this, first reset the ILOM configuration to the default settings and then perform a Restore operation using the known good configuration.
- You want to use the Backup and Restore feature to replicate an ILOM configuration onto other systems. To do this, create a standard ILOM configuration, back up the configuration, edit the backed up XML file to remove settings that are unique to a particular system (for example, the IP address), then perform Restore operations to replicate the configuration onto the other systems.
- You created a minimum ILOM configuration but to make it complete you need to configure a number of users (ILOM supports a maximum of 10 local user accounts). If you have backed up a configuration previously that has the same users, you can edit the XML file so that it only includes the user information and then simply perform a Restore operation to overlay the minimum configuration with the configuration that has the user accounts. Reuse of large network configurations such as Active Directory is another use case for this approach.

You can use either the web interface or the CLI to perform configuration management tasks in ILOM. For more information about these tasks, see:

- "Backup and Restore Operations" on page 45
- "Reset to Defaults Feature" on page 46

Backup and Restore Operations

ILOM supports two separate operations for backup and restore.

- The Backup operation consists of gathering the current ILOM configuration data into an XML file and transferring that file to a remote system.
- The Restore operation consists of retrieving the XML backup file and using it to restore the ILOM SP to the backed up configuration.

Thus you can use Backup and Restore to save the ILOM configuration to a backup XML file, and later restore the backup file to the same system. Further, if you want to use the backup XML file on other systems, you can edit the XML file to remove or change settings that are unique, such as the IP address. The backup XML file is readable and can be edited manually.

Caution – If you are going to restore the edited backup XML file to the same system, you should reset the ILOM configuration to the default settings; otherwise, the restored configuration will simply overlay the current configuration. If you are going to restore the edited backup XML file to others systems that already contain an ILOM configuration, you should erase the ILOM configuration unless you want to overlay the current configuration. To erase the current ILOM configuration, you must reset the ILOM configuration to the default settings. For instructions, see "Reset the ILOM Configuration to Defaults" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*, or in the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

All of the information that can be configured on the system can be backed up. The privileges assigned to the user account that is used to execute the Backup operation determine how much of the configuration is included in the backup XML file. For security reasons, if the user account used to execute the Restore operation has fewer privileges than the account used to create the backup file, some of the configuration might not be restored. For each configuration property that is not restored due to lack of privileges, a log entry is created. Therefore, one way to verify that all the configuration properties were restored is to check the event log.

You can also limit the amount of information included in the backup XML file by using user accounts that have limited privileges. For example, an account assigned the Admin (`a`), User Management (`u`), Console (`c`), Reset and Host Control (`r`), and Read Only (`o`) roles would have full privileges and would create the most complete

configuration backup file. For this reason, it is recommended that user accounts assigned the a,u,c,r,o roles be used whenever you perform Backup and Restore operations.

Configuration Backup and Restore operations do not change the power state of the host operating system. However, both operations cause all sessions on the ILOM SP to be momentarily suspended until the Backup or Restore operation completes. A Backup or Restore operation typically lasts two to three minutes, after which all logged in sessions resume normal operation.

For instructions on performing Backup and Restore operations and editing a backup XML file, see "Backing Up and Restoring ILOM Configuration" in the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Reset to Defaults Feature

With the Reset to Defaults feature in ILOM, you can reset the ILOM configuration settings to their default settings. When you use this feature you are given three options:

- **All** – Select this option if you want to erase the existing ILOM configuration file. When the ILOM SP reboots, the configuration file that was included in the SP firmware is used instead.
- **Factory** – Select this option if you want to erase the existing configuration file and the internal log files. When the ILOM SP reboots, the configuration file that was included in the SP firmware is used instead and the internal log files are erased.
- **None** – Select this option if you want to cancel the reset operation you initiated previously. To cancel a previously initiated reset operation you must initiate a reset operation with the None option before the ILOM SP reboots.

Note – When you execute an ILOM configuration reset, the reset configuration does not take effect until the ILOM SP reboots.

For instructions on resetting the ILOM configuration to the default settings, see "Reset the ILOM Configuration to Defaults" in the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

ILOM Firmware Updates

All ILOM firmware releases are available for download from the official Sun download page for your server platform.

New versions of firmware typically offer new features and product enhancements. To ensure that you have the latest improvements, it is highly recommended that you update the firmware on your system with the latest firmware release that is available.

Updating the firmware on your system to a prior release is *not* recommended. However, if you determine you need to run an earlier version of the firmware on your system, you can update the firmware to any prior firmware release that is available for download.

To determine the URL of the Sun download page for your server, refer to the platform-specific ILOM Supplement.

Identification of ILOM Version Information

Prior to updating the ILOM firmware, you should identify the ILOM firmware version that is running on the server SP or CMM.

If you determine that you have ILOM 2.x installed on your system (server SP or CMM) and you are updating to a later ILOM 2.x version, you need to refer to the *Sun Integrated Lights Out Manager 2.0 User's Guide* to find the firmware update procedures for ILOM 2.x.

If you are updating to ILOM 3.x, you need to refer to the procedures for updating ILOM firmware in one of the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Process for Updating the Firmware

The process for updating the firmware version installed on your Sun server or CMM involves:

1. Downloading the firmware image for your server or CMM from the Sun platform's product web site.
2. Copying the image to a server using a supported protocol (FTP, TFTP, HTTP, HTTPS). For a CLI update, copy the image to a local server. For a web interface update, copy the image to the system on which the web browser is running.
3. If required by your platform, shut down the host operating system before changing the firmware on your server SP.
4. Logging in to ILOM using an Admin (a) role account.
5. Loading the firmware image on the server SP (or CMM) using the ILOM CLI or the web interface.
6. Optionally, preserve the current configuration in ILOM. For more information, see "Preserve Configuration Option" on page 48
7. Verifying that the appropriate firmware version was installed after the system reboots.

Preserve Configuration Option

When updating to a later firmware release, the Preserve Configuration option (when enabled) saves your existing configuration in ILOM and restores the configuration after the update process completes.

Note – The term *configuration* refers to the settings configured in ILOM by a user. These settings can include user management settings, SP network settings, serial port settings, alert management configurations, remote management configurations, and so on.

If you are updating to a prior firmware release and ILOM detects a preserved configuration for that release, the Preserve Configuration option (when enabled) reverts to the configuration for the prior release after the update process completes.

For example: If you update your system firmware from 3.0 to 2.0 and choose to enable Preserve Configuration during the update process, ILOM will:

- Determine whether a snapshot of the 2.0 configuration was previously preserved on the system.
- Restore the snapshot of the 2.0 configuration, if found, after the update process completes.

However, in this example, if ILOM is unable to locate the snapshot of the 2.0 configuration, ILOM will not restore the 2.0 configuration. After the update process completes, the configuration will revert to the system defaults.

Troubleshoot an Update Session If Network Failure Occurs

If you were performing the firmware update process using the ILOM web interface or CLI and a network failure occurs, ILOM will *not* reboot. You should *not* reboot the system. However, you should do the following:

1. Address and fix the network problem.
2. Reconnect to the ILOM SP.
3. Restart the update process.

CHAPTER 7

Remote Host Management Options

Topics

Description	Links
Identify the remote management options	• "Remote Management Options" on page 52
Learn about controlling the power state of a remote server	• "Power Control" on page 52 • "ILOM CLI – Remote Power Commands" on page 53 • "ILOM Web Interface – Remote Power Controls" on page 53
Learn about diagnostic tests	• "Diagnostics for x64 or SPARC Systems" on page 54
Learn about redirecting storage media from the CLI on your local system to a remote host server	• "Storage Redirection CLI" on page 55 • "First Time Access" on page 55 • "Storage Redirection CLI Architecture" on page 56 • "Default Network Communication Port" on page 57
Learn about redirecting devices (keyboard, video display, mouse, storage) from the web interface on your local system to a remote host server	• "Sun ILOM Remote Console" on page 57 • "Single or Multiple Remote Host Server Management Views" on page 58 • "Installation Requirements" on page 60 • "Network Communication Ports and Protocols" on page 61 • "Sign In Authentication Required" on page 61 • "CD and Diskette Redirection Operation Scenarios" on page 62

Related Topics

For ILOM	Chapter or Section	Guide
• CLI	• Managing Remote Hosts	*Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* (820-6412)
• Web interface	• Managing Remote Hosts	*Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at:
http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

Remote Management Options

As of ILOM 3.0, the remote management options in ILOM include:

- Power control
- Diagnostic configuration
- Storage Redirection Command-Line Interface (CLI)
- Sun ILOM Remote Console (graphical interface)

Information about each of these remote management options follows.

Power Control

The remote power control options in ILOM are available for all Sun servers from the ILOM CLI or web interface. These options enable you to control the power state of a remote host server.

ILOM CLI – Remote Power Commands

From a command window or terminal, you can issue the following commands to remotely control the power state of a host server:

- **`start`**. Use the `start` command to turn on full power to the remote host server.

  Example: -> `start /SYS`

- **`stop`**. Use the `stop` command to shut down the OS gracefully prior to powering off the remote host server.

  Example: -> `stop /SYS`

- **`stop -f`**. Use the `stop -f` command to immediately turn off the power to the remote host server.

  Example: -> `stop -f /SYS`

- **`Reset`**. Use the `reset` command to immediately reboot the remote host server.

  Example: -> `reset /SYS`

For information about connecting to a host server or issuing commands from the ILOM CLI, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

ILOM Web Interface – Remote Power Controls

Select the Remote Control --> Remote Power Control tab in the ILOM web interface to remotely control the power state of a host server. The following options are available:

- **Immediate Power Off –** This option immediately turns off the power on the remote host server.
- **Graceful Shutdown and Power Off –** This option shuts down the OS gracefully prior to powering off the remote host server.
- **Power On** (default) **–** This option turns on full power to the remote host server.
- **Power Cycle –** This option immediately turns off the power on the remote host server, then applies full power to the remote host server.
- **Reset –** This option immediately reboots the remote host server.

Diagnostics for x64 or SPARC Systems

Diagnostic configuration options in ILOM are available on some Sun servers. These options are accessible from the Remote Control --> Diagnostics tab in the ILOM web interface or by using the CLI. Refer to your platform ILOM Supplement for information about whether your server platform supports these diagnostic options.

- **x64 System - Pc-Check diagnostics options**

  From the Diagnostics tab of the ILOM web interface, you can select any of the following options from the Run Diagnostic on Boot drop-down list box.

  - **Disabled –** Select Disabled if you do not want to run Pc-Check diagnostic tests upon startup of a remote host server.
  - **Enabled –** Select Enabled if you want to run basic Pc-Check diagnostic tests upon start-up of the remote host server. These basic diagnostic tests typically take 5 minutes to complete.
  - **Extended –** Select Extended if you want to run extended Pc-Check diagnostic tests upon start-up of the remote host server. These extended diagnostic tests typically take 20 to 40 minutes to complete.
  - **Manual –** Select Manual if you want to run select Pc-Check diagnostic tests upon start-up of the remote host server.

- **SPARC System Diagnostic Configuration Settings**

  On a Sun SPARC system using ILOM, you can enable the diagnostic mode, specify triggers and the level of diagnostics, as well as the verbosity of the diagnostic output.

- **Generate NMI option (x64 Systems)**

  You can send a non-maskable interrupt (NMI) to the host operating system using either the CLI or the web interface. Note that sending an NMI to the host could cause the host to stop responding and wait for input from an external debugger.

For further instruction on using the diagnostic options in ILOM, see "Diagnosing x64 Systems Hardware Issues" and "Diagnosing SPARC Systems Hardware Issues" in the following guides:

- *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
- *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*

Storage Redirection CLI

The Storage Redirection CLI in ILOM is supported on all Sun x64 processor-based servers. This CLI is also supported on some SPARC processor-based servers. However, the Storage Redirection CLI is not supported on Sun server SPs or chassis monitoring modules (CMMs) running ILOM 2.0. It is also not supported on CMMs running ILOM 3.0.

The Storage Redirection CLI enables the storage devices (CD/DVD or ISO images) on your local client to behave as if they were directly attached to the remote host server. For instance, the redirection functionality enables you to locally perform these actions:

- Mount a storage device or image directly from your desktop to a remote SP host without launching the Sun ILOM Remote Console application.
- Redirect media to use the `/SP/console` for text-based console interaction.
- Write scripts to start and stop storage redirection on multiple SP host servers.

Note – The Storage Redirection CLI is limited to remote media control. If you need to remotely manage other devices on a remote host server (such as the keyboard, video display, or mouse), you should use the Sun ILOM Remote Console. For more information about the Sun ILOM Remote Console, see "Sun ILOM Remote Console" on page 57.

For instructions for using the Storage Redirection CLI, see "Managing Remote Hosts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide.*

First Time Access

When you access the Storage Redirection CLI for the first time, you must sign in to the ILOM web interface to install the service and the client. After the service and client are installed on your system, you can subsequently start the service and launch the Storage Redirection CLI directly from a command window or terminal.

Note – You can, alternatively, choose to start the service directly from the ILOM web interface. If you choose to start the service from the ILOM web interface without installing it, you will need to subsequently access the ILOM web interface to start the service prior to launching the Storage Redirection CLI from a command window or terminal. For more information about how to install or start the service, see "Managing Remote Hosts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Storage Redirection CLI Architecture

The Storage Redirection CLI consists of a Java Web Start service and a scriptable, Java command-line client. You must start the service and initially install the client from the ILOM web interface. The Storage Redirection service runs in the background of your local client and establishes the connection between your local client and the remote host server. After a connection is established, you can locally launch the Storage Redirection CLI from a command window or terminal. The Storage Redirection CLI enables you to issue commands to the service for starting and stopping storage redirection.

FIGURE 7-1 Storage Redirection Service and Client

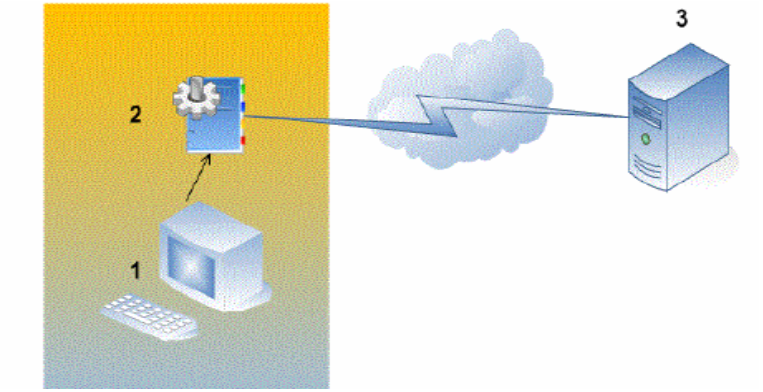


Figure Legend

1	Local client running Storage Redirection command-line client
2	Storage Redirection service running on local client
3	Remote host server

Note – You can only run one instance of the Storage Redirection service on your local system at one time. However, you can launch multiple Storage Redirection CLIs by issuing the Storage Redirection command (`-jar StorageRedir.jar`) from a local command window or terminal.

Default Network Communication Port

The default network communication port provided for Storage Redirection CLI is 2121. This default socket port enables the Storage Redirection CLI to communicate over the network with a remote host server SP. If you need to change the default network port, you must edit the `Jnlpgenerator-cli` file to manually override the default port number (2121).

For more information about how to edit the network port number that is referenced in the `Jnlpgenerator-cli` file, see "Change the Default Storage Redirect Port: 2121" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

Sun ILOM Remote Console

The Sun ILOM Remote Console is supported on all Sun x64 processor-based servers. It is also supported on some SPARC processor-based servers. The Sun ILOM Remote Console is a Java application that you can launch from the ILOM web interface. When you use the Sun ILOM Remote Console, you can remotely redirect and control the following devices on a remote host server:

- Keyboard
- Mouse
- Video console display
- Storage devices or images (CD/DVD, floppy device, ISO image)

The Sun ILOM Remote Console enables the devices on your local client to behave as if they were directly attached to the remote host server. For instance, the redirection functionality enables you to perform any of the following tasks:

- Install software from your local media drive to a remote host server.
- Run command-line utilities on a remote host server from a local client.
- Access and run GUI-based programs on a remote host server from a local client.
- Remotely configure server features from a local client.
- Remotely manage server policies from a local client.
- Remotely monitor server elements from a local client.
- Perform almost any software task from a local client that you normally could perform while sitting at a remote host server.

The Sun ILOM Remote Console supports two methods of redirection: video and serial console. Video redirection is supported on all Sun x64 processor-based servers and some Sun SPARC processor-based servers. Serial console redirection is supported on all SPARC processor-based servers. Serial console redirection is not currently supported on x64 processor-based servers.

For instructions for redirecting host devices using the Sun ILOM Remote Console, see "Managing Remote Hosts" in the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.*

Single or Multiple Remote Host Server Management Views

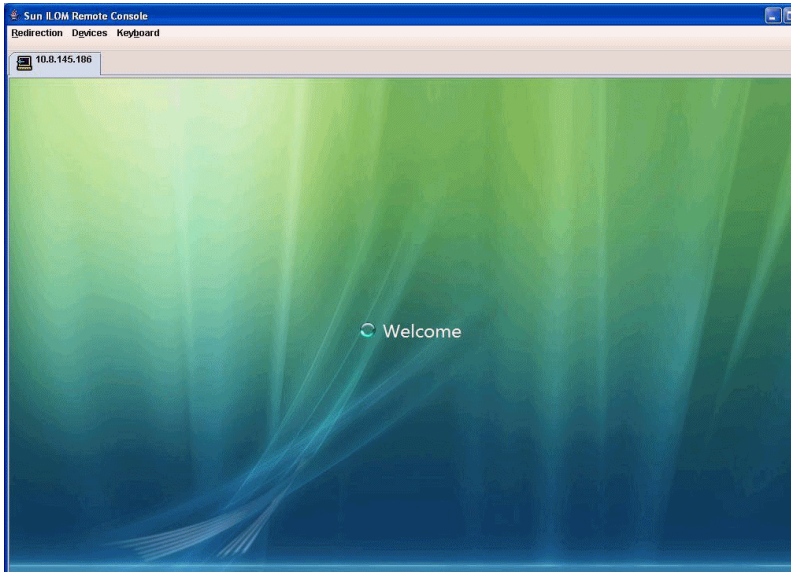
The Sun ILOM Remote Console supports both single and multiple remote server management views.

Single and multiple server management views are currently supported on all x64 processor-based servers and some SPARC processor-based servers.

- **Single Remote Server Management View** – You can launch the Sun ILOM Remote Console to manage a single remote host server from one window and utilize the remote Keyboard, Video, Mouse, Storage (KVMS) features.

  Single remote server management views are supported when you connect to the IP address of any server SP.

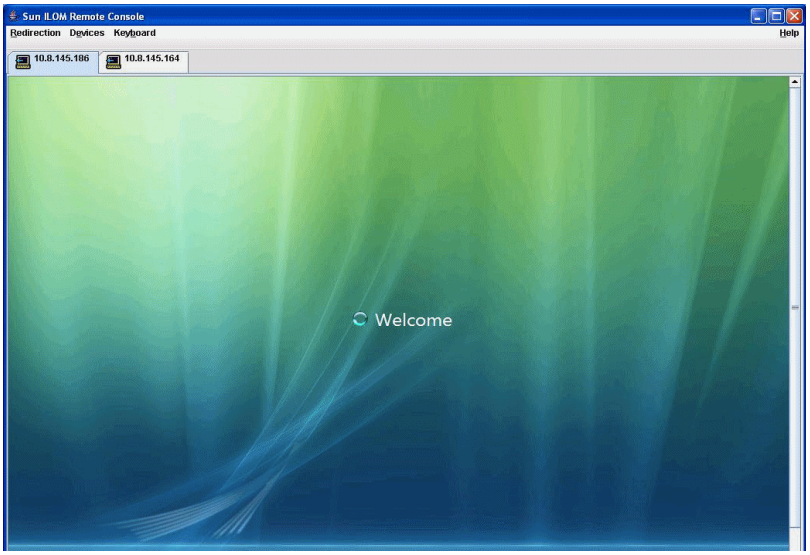
FIGURE 7-2 Single Server Management View



- **Multiple Remote Server Management Views** – You can launch the Sun ILOM Remote Console to manage multiple remote host server views.

  Multiple remote server management views are supported when you either: (1) add a new Sun ILOM Remote Control session to manage another remote host server; or (2) connect to the IP addresses that are associated with an x64 chassis monitoring module (CMM).

FIGURE 7-3 Multiple Server Management Views



Installation Requirements

The Sun ILOM Remote Console does not require you to install any additional hardware or software. It is built into the ILOM software. However, to run the Sun ILOM Remote Console, you must have the JRE 1.5 or higher (Java 5.0 or higher) software installed on your local client. To download the Java 1.5 runtime environment, go to: `http://java.com`

In addition, the Sun ILOM Remote Console is supported on your local client with the operating systems and browsers listed in the following table.

TABLE 7-1 Supported Operating Systems and Web Browsers

Operating System	Web Browser
Solaris (9 and 10)	• Mozilla 1.7.5 and above • Firefox 1.0 and above
Linux (Red Hat, SuSE, Ubuntu)	• Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above
Microsoft Windows (98, 2000, XP, Vista)	• Internet Explorer 6.0 and above • Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above

Network Communication Ports and Protocols

The Sun ILOM Remote Console communicates to a remote host server SP using the following network ports and protocols.

TABLE 7-2 SP ILOM Remote Console Network Ports and Protocols

Port	Protocol	SP - ILOM Remote Console
5120	TCP	CD
5123	TCP	Diskette
5121	TCP	Keyboard and mouse
7578	TCP	Video

Sign In Authentication Required

When you launch the Sun ILOM Remote Console from the ILOM web interface, you must sign in using an Admin (a) or Console (c) role account. The system will subsequently prompt you to reenter the Admin or Console role account each time you perform one of the following: start a redirection, stop a redirection, or restart a redirection.

Note – If the Single Sign On feature is disabled in ILOM, users with Admin (a) or Console (c) role privileges will be prompted to sign in to ILOM again using the Login dialog. For additional information about the Single Sign On feature, see "Single Sign On" on page 22.

CD and Diskette Redirection Operation Scenarios

Use the information in TABLE 7-3 to help identify different case scenarios in which the CD drive or diskette drive redirection functionality might behave during a Remote Console session.

TABLE 7-3 Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD as Seen by Remote Host	Diskette as Seen by Remote Host
1	Remote Console application not started, or Remote Console started but DVD/diskette redirection not started	DVD device present. No medium indication is sent to the host from ILOM when the hosts asks.	Diskette device present. No medium indication is sent to the host from ILOM when the host asks.
2	Remote Console application started with no medium present in the drive	DVD device present. When the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case, since there is no medium, the status is no medium.	Diskette device present. When the host asks (for example, you double-click on a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote Console application started with no medium, then medium is inserted	DVD device present. When the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. When the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote Console application started with medium inserted	Same as case 3.	Same as case 3.
5	Remote Console application started with medium present, then medium is removed	Next command from the host will get a status message indicating medium not present.	Next command from the host will get a status message indicating medium not present.
6	Remote Console application started with image redirection	Same as case 3.	Same as case 3.

TABLE 7-3 Remote Console Operation With DVD Drive and Diskette Drive *(Continued)*

Case	Status	DVD as Seen by Remote Host	Diskette as Seen by Remote Host
7	Remote Console application started with image, but redirection is stopped (which is the only way to stop ISO redirection)	Driver knows DVD redirection stopped, so it sends a medium absent status on the next host query.	Driver knows DVD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure	The software has a keep-alive mechanism. The software will detect keep-alive failure since there is no communication and will close the socket, assuming the client is unresponsive. Driver will send a no medium status to the host.	The software has a keep-alive mechanism. The software will detect unresponsive client and close the socket, as well as indicate to the driver that the remote connection went away. Driver will send a no medium status to the host.
9	Client crashes	Same as case 8.	Same as case 8.

APPENDIX **A**

Example Setup of Dynamic DNS

This appendix describes how to configure the Dynamic Domain Name Service (DDNS) on a typical customer's infrastructure. The instructions and example configuration provided here do not affect ILOM or the service processor (SP).

The following topics are covered in this appendix:

- "Dynamic DNS Overview" on page 65
- "Example Dynamic DNS Configuration" on page 67

Dynamic DNS Overview

Once DDNS is configured, new ILOM systems will be automatically assigned a host name and an IP address at install time. Thus, once you have configured DDNS, clients can use either host names or IP addresses to access any ILOM SPs that have been added to the network.

By default, ILOM systems are shipped with Dynamic Host Configuration Protocol (DHCP) enabled so that you can use DHCP to configure the SP's network interface. With DDNS, you can further leverage DHCP to automatically make the DNS server aware of the host names of ILOM systems that have been added to the network and configured using DHCP.

Note – Domain Name Service (DNS) support, which was added to ILOM in the 3.0 release, allows hosts such as NTP servers, logging servers, and firmware upgrade servers, to be referred to within the ILOM command-line interface (CLI) and other user interfaces by host name or IP address. DDNS support, as described in this appendix, allows SPs to be referred to by their host names without being manually configured.

ILOM systems are assigned well-known host names consisting of a prefix followed by a hyphen and the ILOM SP product serial number. For rackmounted systems and server modules, the host name will consist of the prefix SUNSP and the product serial number. For a server chassis with multiple chassis monitoring modules (CMMs), the host name for each CMM will consist of the prefix SUNCMM*n* and the product serial number, where *n* is 0 or 1. For example, given a product serial number of 0641AMA007, the host name for a rackmounted system or a server module would be SUNSP-0641AMA007. For a server chassis with two CMMs, the host names for the CMMs would be SUNCMM0-0641AMA007 and SUNCMM1-0641AMA007.

Once DDNS has been configured, SP/DHCP/DNS transactions are automatically executed to add new host names and associated IP addresses to the DNS database. Each transaction comprises the following steps:

1. ILOM creates the SP host name using the appropriate prefix and the product serial number and the ILOM SP sends the host name to the DHCP server as part of the DHCP request.
2. When the DHCP server receives the request, it assigns an IP address to the ILOM SP from an available pool of addresses.
3. The DHCP server then sends an update to the DNS server to notify it of the newly configured ILOM SP's host name and IP address.
4. The DNS server updates its database with the new information, thus completing the SP/DHCP/DNS transaction.

Once an SP/DHCP/DNS transaction is completed for a given host name, clients can make a DNS request using that host name and DNS will return the assigned IP address.

To determine the host name of a particular ILOM SP, simply check the product serial number on the outside of the SP itself and combine the product serial number with the appropriate prefix as described above. You can also determine host names by checking the server logs for DNS zone update messages.

Note – You can use the CLI to change the SP host name to something other than the default. However, if you change the host name to a non-default name, clients must use that host name to refer to the SP using DNS.

The DNS information is updated when a DHCP lease renewal causes an IP address change, and the DNS information is deleted when the DHCP lease is released.

Note – For all ILOM SPs that have been assigned host names prior to DDNS support or that may have been configured using DDNS and MAC address-based host names, the previously configured host names will remain in effect.

Example Dynamic DNS Configuration

This section describes how to set up an example DDNS configuration. You can use the procedures and sample files provided here, with site-specific modifications, to set up your own DDNS configuration.

Note – How you set up DDNS depends on the infrastructure in use at your site. Solaris, Linux, and Windows operating systems all support server solutions that offer DDNS functionality. This example configuration uses Debian r4.0 as the server operating system environment.

This following topics are covered in this section:

- "Assumptions" on page 67
- "Configure and Start the DHCP and DNS Servers" on page 67
- "References" on page 69

Assumptions

This example configuration is based on the following assumptions:

- There is a single server that handles both DNS and DHCP for the network the SP resides on.
- The SP network address is 192.168.1.0.
- The DHCP/DNS server address is 192.168.1.2
- The IP addresses from 192.168.1.100 to 192.168.1.199 are used as a pool to provide addresses to the SP and other clients.
- The domain name is `example.com`.
- There is no existing DNS or DHCP configuration in place. If there is, use the following files as a guideline to update the existing configuration.

▼ Configure and Start the DHCP and DNS Servers

To configure the servers, follow these steps:

1. **Install the `bind9` and `dhcp3-server` packages from the Debian distribution.**

   Installing the `dnsutils` package provides access to `dig`, `nslookup` and other useful tools as well.

2. **Using** `dnssec-keygen`**, generate a key to be shared between the DHCP and DNS servers to control access to the DNS data.**

3. **Create a DNS configuration file named** `/etc/bind/named.conf` **that contains the following:**

```
options {
  directory "/var/cache/bind";
  auth-nxdomain no;    # conform to RFC1035
  listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
  type hint;
  file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912
zone "localhost" {
  type master;
  file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
  type master;
  file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
  type master;
  file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
  type master;
  file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
  algorithm HMAC-MD5;
  secret "your-key-from-step-2-here"
};
zone "example.com" {
  type master;
  file "/etc/bind/db.example.com";
  allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.example.rev";
  allow-update { key server.example.com; };
};
```

4. **Add empty zone files for the local network.**

   Empty zone files should be named `/etc/bind/db.example.com` and `/etc/bind/db.example.rev`.

   Copying the distribution supplied `db.empty` files is sufficient; they will be updated automatically by the DNS server.

5. **Create a `/etc/dhcp3/dhcpd.conf` file that contains the following:**

```
ddns-update-style interim;
ddns-updates      on;
server-identifier server;
ddns-domainname   "example.com.";
ignore client-updates;
key server.example.com {
  algorithm hmac-md5;
  secret your-key-from-step-2-here;
}
zone example.com. {
  primary 127.0.0.1;
  key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
  primary 127.0.0.1;
  key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.199;
  option domain-name-servers 192.168.1.2;
}
```

6. **After completing steps 1 through 5 above, run the `/etc/init.d` script to start the DNS and DHCP servers.**

   Once the servers are running, any new ILOM SPs configured for DHCP will be automatically accessible using their host name when they are powered on. Use log files, `dig`, `nslookup`, and other utilities for debugging, if necessary.

References

For more information on the Linux DHCP and DNS servers used in this example, see the Internet Systems Consortium web site at: http://www.isc.org/

APPENDIX **B**

Glossary

A

access control list (ACL) A software authorization mechanism that enables you to control which users have access to a server. Users can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.

Active Directory A distributed directory service included with Microsoft Windows Server operating systems. It provides both authentication of user credentials and authorization of user access levels to networked resources.

actual power The amount of power consumed by all power supplies in the system.

address In networking, a unique code that identifies a node in the network. Names such as "host1.sun.com" are translated to dotted-quad addresses, such as "168.124.3.4" by the Domain Name Service (DNS).

address resolution A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.

Address Resolution Protocol (ARP) A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Administrator The person with full access (root) privileges to the managed host system.

agent A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.

alert A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.

Alert Standard Format (ASF) A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or other excursions and to send Remote Management and Control Protocol (RMCP) alerts according to the Platform Event Trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access-control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.

authenticated user A user that has successfully undergone the process of authentication and has subsequently been granted access privileges to particular system resources.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

available power On a rackmounted server, available power is the sum of all the power that the power supplies can provide. On a server module, available power is the amount of power the chassis is willing to provide to the server module.

B

bandwidth A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.

baseboard management controller (BMC) A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.

baud rate The rate at which information is transmitted between devices, for example, between a terminal and a server.

bind In the Lightweight Directory Access Protocol (LDAP), this refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS (Basic Input/Output System) System software that controls the loading of the operating system and testing of hardware at system power on. BIOS is stored in read-only memory (ROM).

bits per second (bps) The unit of measurement for data transmission speed.

boot loader A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

cache A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA) A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate, and a public key that belongs to that entity, which is also present in the certificate.

chassis monitoring module (CMM) A typically redundant, hot-pluggable module that works with the service processor (SP) on each blade to form a complete chassis management system.

client In the client/server model, a system or software on a network that remotely accesses resources of a server on a network.

command-line interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

console A terminal, or dedicated window on a screen, where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC) The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event A system event that seriously impairs service and requires immediate attention.

customer-replaceable unit (CRU) A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES) A common algorithm for encrypting and decrypting data.

Desktop Management Interface (DMI) A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).

digital signature A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.

Digital Signature Algorithm (DSA) A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.

direct memory access (DMA) The transfer of data directly into memory without supervision of the processor.

directory server In the Lightweight Directory Access Protocol (LDAP), a server which stores and provides information about people and resources within an organization from a logically centralized location.

Distinguished Name (DN) In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

Distributed Management Task Force (DMTF) A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, "sun.com" identifies Sun Microsystems as the owner of the domain in the FQDN "docs.sun.com."

domain name The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as "sun.com." Domain names are interpreted from right to left. For example, "sun.com" is both the domain name of Sun Microsystems, and a subdomain of the top-level ".com" domain.

Domain Name Server (DNS) The server that typically manages host names in a domain. DNS servers translate host names, such as "www.example.com," into Internet Protocol (IP) addresses, such as "030.120.000.168."

Domain Name System (DNS) A distributed name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as "00.120.000.168," with host names, such as "www.sun.com." Machines typically get this information from a DNS server.

Dynamic Domain Name Service (DDNS) A service that ensures that a Domain Name Server (DNS) always knows the dynamic or static IP address associated with a domain name.

Dynamic Host Configuration Protocol (DHCP) A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

E

enhanced parallel port (EPP) A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.

Ethernet An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.

event A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.

external serial port The RJ-45 serial port on the server.

externally initiated reset (XIR) A signal that sends a "soft" reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system in order to reach the console prompt. A user can then generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

failover The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet Ethernet technology that transfers data up to 100M bits per second. Fast Ethernet is backward-compatible with 10M-bit per second Ethernet installations.

Fault Management Architecture (FMA) An architecture that ensures a computer can continue to function despite a hardware or software failure.

field-replaceable unit (FRU) A system component that is replaceable at the customer site.

file system A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below root.

File Transfer Protocol (FTP) A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.

firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

fully qualified domain name (FQDN) The complete and unique Internet name of a system, such as "www.sun.com." The FQDN includes a host server name (www) and its top-level (.com) and second-level (.sun) domain names. A FQDN can be mapped to a system's Internet Protocol (IP) address.

G

gateway A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.

Gigabit Ethernet Ethernet technology that transfers data up to 1000M bits per second.

graphical user interface (GUI) An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

H

host A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

host ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.

host name The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

hot-plug Describes a component that is safe to remove or add while the system is running. However, before removing the component, the system administrator must prepare the system for the hot-plug operation. After the new component is inserted, the system administrator must instruct the system to reconfigure the device into the system.

hot-swap Describes a component that can be installed or removed by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot pluggable, but not all hot-pluggable components are hot-swappable.

Hypertext Transfer Protocol (HTTP) The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Hypertext Transfer Protocol Secure (HTTPS) An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

Integrated Lights Out Manager (ILOM) An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.

Intelligent Platform Management Interface (IPMI) A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors. This enables a management application running on the

operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes Field Replacable Unit (FRU) inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

internal serial port The connection between the host server and ILOM that enables an ILOM user to access the host serial console. The ILOM internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM1, or /dev/ttyS0. Normally, the host serial console settings match ILOM's default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

Internet Control Message Protocol (ICMP) An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.

Internet Protocol (IP) The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.

Internet Protocol (IP) address In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as "192.168.255.256," which specifies the actual location of a machine on an intranet or the Internet.

IPMItool A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Remote Console A console written in Java that allows a user to access an application while it is running.

Java(TM) Web Start application A web application launcher. With Java Web Start, applications are launched by clicking on the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be launched from a desktop icon or browser

K

kernel The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

keyboard, video, mouse, storage (KVMS) A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

lights out management (LOM) Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

Lightweight Directory Access Protocol (LDAP) A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

Lightweight Directory Access Protocol (LDAP) server A software server that maintains an LDAP directory and service queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

local area network (LAN) A group of systems in close proximity that can communicate via connecting hardware and software. Ethernet is the most widely used LAN technology.

local host The processor or system on which a software application is running.

M

major event A system event that impairs service, but not seriously.

Management Information Base (MIB) A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.

man pages Online UNIX documentation.

media access control (MAC) address Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture.

Message Digest 5 (MD5) A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.

minor event A system event that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace and printers are named within the printer namespace.

Network File System (NFS) A protocol that enables disparate hardware configurations to function together transparently.

Network Information Service (NIS) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

network management station (NMS) A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.

network mask A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.

Network Time Protocol (NTP) An Internet standard for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NTP synchronizes the clock times of networked devices with NTP servers to the millisecond using Coordinated Universal Time (UTC).

node An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

nonvolatile memory A type of memory that ensures that data is not lost when system power is off.

O

object identifier (OID) A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.

OpenBoot(TM) PROM A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.

OpenIPMI An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).

Operator A user with limited privileges to the managed host system.

out-of-band (OOB) system management Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

P

parity A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.

Pc-Check An application made by Eurosoft (UK) Ltd. that runs diagnostic tests on computer hardware.

permissions A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.

permitted power The maximum power that the server will permit to be used at any given time.

physical address An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.

Platform Event Filtering (PEF) A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.

Platform Event Trap (PET) A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)-specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.

port The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

port number A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

power cycling The process of turning the power to a system off then on again.

Power Monitoring interface An interface that enables a user to monitor real-time power consumption, including available power, actual power, and permitted power, for the service processor (SP) or an individual power supply with accuracy to within one minute of the time the power usage occurred.

power-on self-test (POST) A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.

Preboot Execution Environment (PXE) An industry-standard client/server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.

Privacy Enhanced Mail (PEM) A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

protocol A set of rules that describes how systems or devices on a network exchange information.

proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

real-time clock (RTC) A battery-backed component that maintains the time and date for a system, even when the system is powered off.

reboot An operating system-level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.

redirection The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.

Remote Authentication Dial-In User Service (RADIUS) A protocol that authenticates users against information in a database on a server and grants authorized users access to a resource.

Remote Management and Control Protocol (RMCP) A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off or forcing a reboot.

remote procedure call (RPC) A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server and the result is transmitted back to the client.

remote system A system other than the one on which the user is working.

reset A hardware-level operation that performs a system power-off, followed by a system power-on.

role An attribute of user accounts that determines user access rights.

root In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.

root directory The base directory from which all other directories stem, either directly or indirectly.

router A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term "router" commonly refers to a device that connects two networks.

RSA algorithm A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.

schema Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

S

Secure Shell (SSH) A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.

Secure Socket Layer (SSL) A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

sensor data record (SDR) To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records. They include software information, such as how many sensors are present, what type they are, their events, threshold information, and so on. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.

serial console A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

serial port A port that provides access to the command-line interface (CLI) and the system console stream using serial port redirection.

server certificate A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).

Server Message Block (SMB) protocol A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on and request services from server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the Common Internet File System (CIFS).

service processor (SP) A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical functions of the SP are to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.

session time-out A specified duration after which a server can invalidate a user session.

Simple Mail Transfer Protocol (SMTP) A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving email.

Simple Network Management Protocol (SNMP) A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.

Single Sign On (SSO) A form of authentication in which a user enters credentials once to access multiple applications.

Snapshot utility An application that collects data about the state of the server processor (SP). Sun Services uses this data for diagnostic purposes.

subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an "address mask."

Sun Blade Modular System A chassis that holds multiple Sun Blade server modules.

Sun Blade server module A server module (blade) that can be plugged into a chassis, also known as a modular system

Sun ILOM Remote Console A graphical user interface that enables a user to redirect devices (keyboard, mouse, video display, storage media) from a desktop to a remote host server.

superuser A special user who has privileges to perform all administrative functions on a UNIX system. Also called "root."

syslog A protocol over which log messages can be sent to a server.

system event log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor or directly with event messages sent from the host.

system identifier A text string that helps identify the host system. This string is included as a varbind in SNMP traps generated from the SUN-HW-TRAP-MIB. While the system identifier can be set to any string, it is most commonly used to help identify the host system. The host system can be identified by a description of its location or by referencing the host name used by the operating system on the host.

T

Telnet The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.

threshold Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.

time-out A specified time after which the server should stop trying to finish a service routine that appears to be hung.

transmission control block (TCB) Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP) An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.

trap Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.

Trivial File Transport Protocol (TFTP) A simple transport protocol that transfers files to systems. TFTP uses User Datagram Protocol (UDP).

U

Uniform Resource Identifier (URI) A unique string that identifies a resource on the Internet or an intranet.

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 450M bits per second (USB 2.0). A USB port connects devices, such as mouse pointers,

user account A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Datagram Protocol (UDP) A connectionless transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, via IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.

user privilege levels An attribute of a user that designates the operations a user can perform and the resources a user can access.

user identification (userid) A unique string identifying a user to a system.

user identification number (UID number) The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.

user name A combination of letters, and possibly numbers, that identifies a user to the system.

W

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP/HTTPS and other protocols, and executes server-side programs.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index

A

Active Directory, 23
  determining user authorization levels, 23
  overview, 23
  user authentication/authorization, 23
active ILOM sessions supported, 14
Admin user account, 7
Administrator privileges, 8
Advanced roles
  capabilities of each role, 6
alerts
  defining an alert rule, 34, 37
  managing from CLI, 36
  managing from SNMP host, 38
  managing from web interface, 37
  specifying destination, 35
  types of levels, 35
  types supported, 33, 34
  warnings for system failures, 33
Altiris Deployment Server, 3
authentication
  using Active Directory, 23
  using LDAP, 24
  using RADIUS, 25
  using SSH host keys, 22
available power, 40

B

Backup and Restore
  recommended roles to use, 45
  sessions momentarily suspended, 46
  use cases, 44
  when to reset to default settings, 45
backup XML file
  editing, 45
  limiting information included, 45
BIOS configurations
  updating, 3
browsers
  supported by Remote Console, 60

C

chassis monitoring module (CMM)
  managing with ILOM, 9
clock settings, 31
collecting data for Sun Services, 32
command-line interface (CLI) capabilities, 8
configuration management
  performing tasks, 44
connecting to ILOM, 14
Console user account, 7

D

data network
  compared to management network, 14
default user account, 11
device redirection
  behavior during Remote Console session, 62
DHCP
  lease release, 66
  lease renewal, 66
  uses, 65
diagnostics

for SPARC systems, 54
for x64 systems, 54
DNS database, 66
dnssec-keygen, 68
documentation for ILOM, vii
Domain Name Service (DNS), 65
downloadable firmware updates, 4
Dynamic DNS
configuration assumptions, 67
configuration example, 67
configuring DHCP and DNS, 67
Debian r4.0 environment, 67
dnssec-keygen, 68
host name, determining, 66
MAC address-based host names, 66
operating systems supported, 67
overview, 65
transaction, description of, 66
well-known host name, 66
Dynamic Domain Name Service
See Dynamic DNS
Dynamic Host Configuration Protocol (DHCP)
uses, 65

E

Email Notification alerts, 34
ENTITY-MIB, 9
Error and fault management, 5
establishing intial communication
initial setup worksheet, 15
Ethernet connection to ILOM, 15
Ethernet management port
connecting to ILOM, 14
event log
capturing timestamps, 31
types of events displayed, 31

F

fault management
monitoring and diagnosing hardware, 30
firmware
about versions, 47
downloading a release, 47
preserving configuration, 48
troubleshooting, 49
update process, 48
update sign-in authentication, 48
updating, 3

H

hardware and FRU inventory, 4
hardware configuration maximum power, 40
host name
assigned using DDNS, 14
assigning, 15
host name format and contents, 66
HP OpenView, 3
HP Systems Insight Manager, 3

I

IBM Director, 3
IBM Tivoli, 3
ILOM 2.x
Administrator
privileges, 8
Operator
privileges, 8
user accounts
compatibility with ILOM 3.0, 8
ILOM configuration
data included in XML backup file, 45
editing XML backup file, 44
replicate configuration, 44
restore to good configuration, 44
when to erase during Restore operation, 45
ILOM service processor
embedded operating system, 2
management capabilities, 9
init.d script, 69
initial login to ILOM, 10
input power, 40
Integrated Lights Out Manager (ILOM)
capabilities, 2
connecting to, 14
description, 2
features and functionality, 4
firmware updates, 47
initial setup, 15
integrating with other management tools, 3
interfaces to, 8
new 3.0 features, 5
roles assigned to accounts, 6, 21
system monitoring features, 28

user interfaces supported, 3, 8
version information, 47
Intelligent Platform Management Interface (IPMI)
capabilities, 9
interfaces to ILOM, 8
inventory and component management, 11
IPMI PET alerts, 34

L

LDAP/SSL
overview, 25
LEDs
when illuminated by ILOM, 29
Lightweight Directory Access Protocol (LDAP)
overview, 24
used for authentication, 24
log in to ILOM
using root user account, 10
using root user account password, 10

M

management network
compared to data network, 14
overview, 14
MIBs supported, 9

N

network connection
using network management port, 14
using serial management port, 14
network failure
during firmware update, 49
network ports used by ILOM, 16
NMI generation, 54
nslookup, 69

O

operating systems
supported by Remote Console, 60
Operator privileges, 8
out-of-band management, 2
output power, 40

P

Pc-Check diagnostics, 54
permitted power, 41
power control
using CLI, 53
power monitoring terminology, 40
power policy setting, 41
Preserve Configuration option
when to use, 48
privileges for user accounts, 6

R

RADIUS
client-server model, 25
overview, 25
used for authentication, 25
Read Only user account, 7
remote access, 4
Remote Console
about, 57
capabilities, 8
installation requirements, 60
network ports and protocols, 61
redirecting CD or diskette, 62
sign-in authentication, 61
single and multiple server views, 58
supported operating systems and browsers, 60
remote diagnostic configuration
about, 54
remote hardware monitoring, 4
remote management options
about, 52
remote power control
about, 52
CLI commands, 53
using CLI, 53
using web interface, 53
Reset and Host Control user account, 7
Reset to Defaults operation
options, 46
use cases, 44
Restore operation
checking the event log, 45
effect of user privileges, 45
verifying data restored, 45
roles for user accounts, 6
root user account, 10

S

sensor readings
  monitoring and diagnosing faults, 30
  types of data reported, 28
serial connection to ILOM, 15
serial management port
  connecting to ILOM, 15
service processor (SP)
  managing with ILOM, 9
Service Snapshot utility, 32
Service user account, 7
sign-in authentication
  required for Remote Console, 61
Simple Network Management Protocol (SNMP)
  capabilities, 9
  configuring alert rules, 38
  MIBs supported, 9
Single Sign On
  overview, 22
  when launching the Remote Console, 61
SNMP Trap alerts, 34
SNMP-FRAMEWORK-MIB, 9
SNMP-MPD-MIB, 9
SNMPv2-MIB, 9
SSH key-based authentication, 22
Storage Redirection CLI
  architecture, 56
  network communication port, 57
  overview, 55
Sun Services
  using Service Snapshot utility, 32
Sun xVM Ops Center
  using with ILOM, 3
SUN-HW-TRAP-MIB, 9
SUN-ILOM-CONTROL-MIB, 9
SUN-ILOM-PET-MIB, 9
SUN-PLATFORM-MIB, 9
syslog logging utility, 32
System alerts, 5
system identifier
  assigning, 15
system indicators
  customer changeable states, 30
  illuminating conditions, 29
  states, 29
  system assigned states, 30
system monitoring features
  overview, 28
system power control and monitoring, 4
system registration, ix

T

third-party management tools, 3

U

updating ILOM firmware
  preserve configuration option, 48
  process for, 48
  to a new release, 47
  to a previous release, 47
  troubleshooting, 49
user accounts
  assigning roles, 6
  authentication, 20
  configuring, 5
  default user account, 11
  guidelines for managing, 20
  number of accounts supported, 20
  privileges assigned, 21
  roles assigned, 21
  root user account, 10
  specifying names for, 20
  support for ILOM 2.x, 8
User Managerment user account, 7

V

version information
  identifying, 47

W

web interface capabilities, 8

X

XML file
  used for Backup and Restore operations, 45